NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

FIRST RESPONDER IDENTITY MANAGEMENT: POLICY OPTIONS FOR IMPROVED TERRORISM INCIDENT RESPONSE

by

Mark R. Landahl

September 2006

Thesis Advisor: Robert Bach
Second Reader: Anthony Cieri

Approved for public release; distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2006	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: First Responder Identity Management: Policy Options for Improved Terrorism Incident Response			**5. FUNDING NUMBERS**
6. AUTHOR(S) Mark R. Landahl			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) Frederick County Sheriff's Office 110 Airport Drive East Frederick, MD 21701			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

The analysis of domestic incidents of terrorism has revealed many gaps in our Nation's capability to effectively manage the multi-jurisdictional response. Although many gaps have been addressed through implementation of measures based on lessons learned, the most pervasive unresolved issue remains the ability to properly identify first response personnel on incident scenes. The nature of incidents of terrorism requires force protection to be a priority because of the threat of a secondary attack. Identity must be established and authenticated to protect responders and prevent infiltration to perpetrate a secondary attack. This thesis examines and evaluates several options for closing this pervasive identity management capability gap. The current decentralized identity system, a defined and typed response resource for identity management, and the federal identity project initiated under HSPD-12 are examined and evaluated as mechanisms for improving on-scene identity management in the response to incidents of terrorism. The thesis argues the development of a standardized nationwide responder identity token that can be rapidly authenticated and establishing dedicated identity management response resources are essential to improving the response multi-jurisdictional and catastrophic incidents of terrorism.

14. SUBJECT TERMS Identity Management, Identity Management Team, Credentialing, Terrorism Incident Response, Smart Card, Identity Authentication			**15. NUMBER OF PAGES** 95
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited.

FIRST RESPONDER IDENTITY MANAGEMENT: POLICY OPTIONS FOR IMPROVED TERRORISM INCIDENT RESPONSE

Mark R. Landahl
Corporal, Frederick County Sheriff's Office, Frederick, Maryland
B.A., State University of New York College at Cortland, 1996

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN NATIONAL SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
September 2006**

Author: Mark R. Landahl

Approved by: Dr. Robert Bach
Thesis Advisor

Mr. Anthony Cieri
Second Reader

Dr. Douglas Porch
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The analysis of domestic incidents of terrorism has revealed many gaps in our Nation's capability to effectively manage the multi-jurisdictional response. Although many gaps have been addressed through implementation of measures based on lessons learned, the most pervasive unresolved issue remains the ability to properly identify first response personnel on incident scenes. The nature of incidents of terrorism requires force protection to be a priority because of the threat secondary attack. Identity must be established and authenticated to protect responders and prevent infiltration to perpetrate a secondary attack. This thesis examines and evaluates several options for closing this pervasive identity management capability gap. The current decentralized identity system, a defined and typed response resource for identity management, and the federal identity project initiated under HSPD-12 are examined and evaluated as mechanisms for improving on-scene identity management in the response to incidents of terrorism. The thesis argues the development of a standardized nationwide responder identity token that can be rapidly authenticated and establishing dedicated identity management response resources are essential to improving the response multi-jurisdictional and catastrophic incidents of terrorism.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

The completion of this project was not without the assistance of many people, and I'm sure it required unseen divine intervention. First, I would like to thank Frederick County Sheriff James Hagy for sponsoring me for this program, entrusting me with the development of our homeland security programs, and restoring my faith in elected officials. The guidance you have given and example you have set will stay with me forever.

I would also like to thank the faculty and staff of the Center for Homeland Defense and Security. I don't know how I slipped under the wire to get there, but the efforts and energy of the faculty have directly impacted homeland security in Frederick County, Maryland. Our small, but critical, home has benefited from the knowledge and experience of the CHDS faculty in the implementation of many projects that started as an idea in the classroom in Monterey. I thank you on behalf of the citizens of Frederick County who will continue to benefit from your efforts. Thank you to Bob Bach and Tony Cieri for providing the guidance necessary to see the thesis through to the end.

Finally and most importantly, thanks to my family. Charlotte, thank you for your unending patience, willingness to share your husband with a laptop computer, and for listening to hours of discussion about incident response and smart card technology, which you know more about than any other kindergarten teacher in America. Thank you for your love and support. I will make it up to you someday. Casey, thank you for sharing your daddy, and for the hugs that seemed to come when they were most needed to get me through. Also to my parents, Mom thanks for listening and listening, and Dad, I know you're here in spirit…..Look what we've accomplished!

THIS PAGE INTENTIONALLY LEFT BLANK

I. OVERVIEW

A. INTRODUCTION

The date is July 17, 1996. Emergency services personnel from Suffolk County, NY and the United States Coast Guard respond to a report of a catastrophic explosion and crash of a passenger airliner over the ocean off the southern coast of Long Island. The initial assumption is a nexus to terrorism. The East Moriches Coast Guard Station is designated as the operations command post, staging area, and evidence collection point. As the incident shifts from response to recovery, personnel from various response disciplines and levels of government stream into the station. Among them is Lieutenant Colonel David Williams of the U.S. Army Reserve. LTC Williams, dressed in his U.S. Army Reserve flight suit, presents identification, enters the site, and assists in the operation by landing helicopters on the designated helipads. On the third day of his work, LTC Williams is questioned concerning his identity and affiliation. Following a brief investigation, LTC Williams is identified as an impostor, escorted from the property, and charged by the Suffolk County Police.[1]

Identity is defined as the "the collective aspect of the set of characteristics by which a thing is definitively recognizable or known."[2] In the incident described above, the set of characteristics that assumed an identity consisted of a uniform, unverifiable paper credentials, and a demeanor consistent with a military officer. These characteristics allowed the impostor to pass a brief security inspection and work within a 'secured' site for several days. This incident highlights the need for a stronger method of identity verification. The infiltration of the Flight 800 response and recovery operation evidences only one of several dimensions of a comprehensive identity management capability gap for terrorism incident response and recovery operations.

The current identity management system for first responders has left a nation-wide capability gap. The decentralized system has resulted in as many different forms of first responder identification as there are federal agencies, and state and local

[1] Joe Haberstroh and Steve Wick, "Military Impostor Fools Coast Guard," *New York Newsday* (27 July 1996).

[2] *The American Heritage Dictionary of the English Language*, 4th ed., s.v. "Identity."

governments. The lack of standardization and interoperability among forms of identification is problematic when confronting a large-scale, multi-jurisdictional response to a suspected incident of terrorism. In addition to the response to the crash of TWA Flight 800, this lack of capability is documented in the after-action reports of the response to every major domestic incident of terrorism, specifically the 1995 Oklahoma City Bombing and the 9/11 responses to both the World Trade Center and the Pentagon. In the following sections, specific cases will be examined that highlight this pervasive problem and support the implementation of a comprehensive first responder identity management framework that provides identity authentication, training and capability levels, on-scene personnel accountability, and protection from secondary attack.

The question for research is: What is the best policy option to close the first responder identity management capability gap? Three policy options will be analyzed, including the current decentralized identity management system, Identity Management Teams for Incident Response, and First Responder Identity Smart Cards. The results of this research can be utilized to inform policy decisions regarding the closure of the identity management capability gap for terrorism incident response and recovery operations.

B. METHODOLOGY

The analysis presented in this thesis compares three policy options for closing the identity management capability gap along six evaluative dimensions. Four of these dimensions were derived from the review of after-action reports of the response to suspected and confirmed incidents of terrorism. In each case, the reports highlighted identity management deficiencies for incident response. The remaining dimensions are derived from traditional public policy concerns. Three alternative approaches to identity management are evaluated across these criteria to determine the best identity management policy option for improving terrorism incident response.

C. PROBLEM DEFINITION: LESSONS LEARNED ABOUT IDENTITY MANAGEMENT FROM TERRORISM INCIDENT RESPONSE

The identity management capability gap for terrorism incident response is a pervasive but solvable problem. The post 9/11 focus on the development of capabilities related to incident response, including acquisition of CBRNE (Chemical, Biological,

Radiological, Nuclear, Explosive) detection equipment, response apparatus, and personal protective equipment have left out the essential component of identity management. Despite the glaring lack of capability, it has been all but ignored in homeland security preparedness efforts targeted at first response personnel.

Discussion of identity management is also hampered by the absence of an extensive body of knowledge or current debate on the issue. This section begins to address this shortcoming by examining the question, is first responder identity management really a problem? Current accessible information bulletins and the After-Action Reports (AAR) of the response to domestic incidents of terrorism will be examined to develop the answer to this essential question.

The problem of identity management for terrorism incident response begins prior to the TWA Flight 800 disaster and has several dimensions beyond simple authentication of personal identity. The problem was identified in the response to the nation's first major domestic terrorist incident: the bombing of the Murrah Federal Building in Oklahoma City, OK. On April 19, 1995, Timothy McVeigh detonated 4800 lbs. of Ammonium Nitrate mixed with fuel oil loaded in a Ryder box truck outside the Murrah Federal building. The blast caused a catastrophic collapse of the building resulting in the deaths of 168 people and injuries to 500 others. The ensuing public safety response and recovery efforts revealed major gaps in identity management capabilities at all levels of government.

Within two hours of the blast, the Oklahoma City Police Department (OCPD) had established a controlled perimeter around the incident site.[3] Identification of personnel immediately became an issue. Initially, the OCPD moved its Permit and Identification section equipment to the scene to issue identification badges. The operation lasted only a few hours as supplies were quickly exhausted.[4] The OCPD continued to issue alternative forms of identification. Due to rain and lighting conditions, the location of the identity station changed three times. When agents from the Federal Bureau of Investigation (FBI) arrived, they also began issuing identification, causing confusion for those manning the

[3] City of Oklahoma City, *Alfred P. Murrah Federal Building Bombing April 19, 1995: Final Report* (Stillwater, OK: Fire Protection Publications, 1996) , 369.

[4] Ibid, 39.

perimeter. FBI and OCPD finally consolidated their operations and issued one form of identification, operating from a vacant warehouse building. The building was large enough to hold the up to 100 people who were waiting for identification after filling out permit forms and completing necessary identification checks. The combined identification operation issued approximately twenty thousand passes over a seventeen-day period.[5] In the publication *Oklahoma City – Seven Years Later: Lessons Learned for Other Communities*, an unnamed Oklahoma City Law Enforcement Officer claimed: "Over 28,000 identity badges were issued during the Oklahoma City response and recovery effort. It took days to establish a central issuing agency. A predetermined ID system would have greatly reduced ID chaos."[6] Included among the lessons learned of the document is the important recommendation to "Establish a Site ID System…Controlling access to the site is an immediate and on-going need."[7]

The need for a comprehensive identity management solution was also evident in the 9/11 response to the Pentagon. Understanding the lessons learned from the 1995 Oklahoma City bombing, the Arlington County Police Department pre-planned an identification system for incident scene security and accountability. The system consisted of 2,000 colored wristbands to be used for entry to an incident scene. In the tremendous public safety response to the terrorist attack at the Pentagon, Arlington County deployed its identity management system two days into the response. Once the system was utilized, the wristband supply was exhausted within two hours.[8]

The on-scene identity management efforts that followed included a system that took up to two hours to process and provide credentials to relief crews for entry into the site because of limited computers and lack of a central database.[9] The lack of a comprehensive identity management system also led one Arlington County firefighter to

---

[5] City of Oklahoma City, *Alfred P. Murrah Federal Building Bombing April 19, 1995: Final Report*, 219-220.

[6] Oklahoma City National Memorial Institute for the Prevention of Terrorism, *Oklahoma City- Seven Years Later: Lessons Learned for Other Communities* (Oklahoma City: MIPT, 2002), 11.

[7] Ibid, 10.

[8] Titan Systems Corporation, *Arlington County: After Action Report on the Response to the September 11 Terrorist Attack at the Pentagon* (Arlington, VA: n.d.), C-23.

[9] Ibid, A-69.

observe, "A volunteer firefighter tee shirt was the only required identification."[10] At the request of the incident commander, the United States Secret Service instituted a more efficient credentialing system several days into the response.

The identity management recommendations from the Pentagon AAR are similar to the lessons learned first reported in the Oklahoma City AAR. The Pentagon AAR concluded, "Arlington County should work with…emergency response and volunteer organizations to implement a uniform identification system. Such a system should be in place and used routinely…"[11] These incidents indicate the need for a comprehensive identity management system that delivers the necessary capabilities to support incident response operations.

The September 11, 2001 response to World Trade Center terrorist attacks is not documented by an official after-action report and, as a result, there is limited documented information concerning identity management at the incident scene. The McKinsey & Co. report prepared for the New York City Police Department entitled *Improving NYPD Emergency Preparedness and Response* does provide some information regarding the problems associated with identification on the WTC incident scene.

The report asserts that it took several days to secure the perimeter. It also details the problems caused by this delay. The report states that "due to inconsistent control of access and absence of an effective credentialing system, perimeter security not adequately established, allowing large numbers of unnecessary personnel to enter site."[12] Although the report does not contain a sanctioned set of recommendations or lessons learned, the challenges faced during the response and recovery operation can be discerned from the content of the report. Based on the evidence provided above, it can be discerned that perimeter security and identity management proved to be significant challenges without an effective solutions.

The previous sections identify many of the gaps associated with past responses to domestic terrorism incidents. Knowing identity management is a problem, in the past

[10] Titan Systems Corporation, *Arlington County*, A-20.

[11] Ibid, C-28.

[12] McKinsey & Company, *Improving NYPD Emergency Preparedness and Response* (New York: McKinsey & Company, 2002), 17.

and in the future, but avoiding steps to solve, would once again demonstrate that the nation suffers from a "failure of imagination" as described in the *9/11 Commission Report*.[13] If we reasonably know what is possible, it should be included in our planning and preparation.

The opening vignette revealed the ability to exploit current identity documents for secure site infiltration. This gap could be exploited to perpetrate a secondary attack. In *Improving NYPD Emergency Preparedness and Response* it is identified that the "risk of secondary attack was not made a priority."[14] This reveals that the possibility of secondary attack at incident scenes such as the WTC response must be considered. The May 2005 issue of the FBI Law Enforcement Bulletin identifies the two components of a secondary attack as follows: "The first one draws in emergency responders, regardless of the extent of deaths and injuries. In the second, the responders themselves become the target and include not only law enforcement, fire and rescue, and emergency medical personnel but civilian Good Samaritans as well."[15]

The exploitation of unverifiable identity to perpetrate a secondary attack is a plausible conclusion based on its pervasive failures in previous incident response. The utilization of this gap for terrorist activity is also advanced by the Department of Homeland Security and Federal Bureau of Investigation joint bulletin released in December 2004 titled *Potential Terrorist Use of Public Safety or Service Industry Uniforms, Identification, or Vehicles*.[16] The bulletin warns of the potential exploitation of the unverifiable identity characteristics of the public safety and service industry (uniforms, paper identification, vehicles, etc.) for terrorist activity. Possible scenarios include the use public safety and service industry uniforms or vehicles to perpetrate a

---

[13] National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States* (New York: Norton & Co, 2004), 336.

[14] McKinsey & Company, *Improving NYPD Emergency Preparedness and Response*, 17.

[15] Brian Houghton, and Jonathan Schacter, "Coordinated Terrorist Attacks Implications for Local Responders," *FBI Law Enforcement Bulletin* 74, no. 5 (May 2005), htttp://www.fbi.gov/publications/leb/2005/may2005/may05/leb.htm#page11/ [accessed January 15, 2006].

[16] U.S. Department of Homeland Security and the Federal Bureau of Investigation, *Information Bulletin: Potential Terrorist Use of Public Safety or Service Industry Uniforms, Identification, or Vehicles* (Washington, D.C.: DHS, n.d.), 1-4, http://www.iafc.org/associations/4685/files/DHSFBI%20alert.pdf. (accessed 10 June 2006).

secondary attack on first responders. The exploitation of these unverifiable identity characteristics could allow access to critical sites, such as staging areas, where a secondary attack would prevent rescue efforts and potentially cause mass casualties to first responders. Although a secondary attack can also come from a pre-placed device, the possibility exists for an attack precipitated by infiltration through the unverifiable flash identification, uniform, and vehicle paradigm.

The after-action and related reports detailing the response to the three major domestic terrorist attacks reveal a common problem that, to date has not been effectively resolved. The common element among the lessons learned from the responses to each incident reveals that identity management failure is endemic to terrorism incident response. From Oklahoma City, OK to Arlington, VA to New York City, NY, identity management is a glaring response capability gap. Despite AAR recommendations regarding improvements needed in identity management dating back to 1995, little has been accomplished toward the recognition and development of a solution. Identity management is not simply a local, state, or regional problem, but a national problem that has been largely ignored.

D. THE CHALLENGE: EVALUATING AND CHOOSING THE BEST IDENTITY MANAGEMENT APPROACH

The definition of the identity management problem for incident response leads to a second, equally critical question; what is an appropriate set of criteria with which to evaluate the effectiveness of identity management solutions? The evaluative criteria defined below are derived from two different perspectives. First, the criteria reflect gaps exposed through the analysis of the response to previous incidents of terrorism and the consideration of future incident scenarios. Second, the criteria include traditional public policy concerns. These two sources of criteria serve to balance a theoretical solution of improving incident response with the realities of the implementation of public sector programs. The purpose of the following sections is to examine these evaluative criteria in more detail as an introduction to analyses presented later in the thesis.

1. Criteria for Evaluation: Failures of Identity Management for Terrorism Incident Response

The collective experiences from the response to major incidents of terrorism detailed above reveal common problems for identity management and terrorism incident

response. The problems as identified and defined provide the framework for a solution. The common problems exposed in the analysis form the basis of the criteria for the evaluation of alternatives to improve identity management for terrorism incident response. These diagnosed problems of the past are then coupled with the possibilities for future response to ensure proper evaluation of alternative solutions.

The four criteria described in this section provide the evaluative elements necessary to improve terrorism incident response. These elements, when included with the additional criteria contained in the following section, form the basis for effective evaluation of alternative approaches to solving the problem posed by on-scene identity management for terrorism incident response.

a. Identity Authentication

In *Identity Fraud: A Critical National and Global Threat*, the key to identity authentication is described as "access to data to assist in the validation, verification, and authentication of personal identifiers."[17] Validation of the data is predicated on trust. The heart of identity management lies in the creation and maintenance of trust. Trust allows for a consumer to have a defined level of certainty in the authenticity of a credential based on the process by which it was issued and the security of the token. The trust model provides a level of certainty to the consumer to answer the question, "Who is this?" Certainty and trust are measured through a two-pronged test of product and process.

In order to provide certainty and trust in an identity credential, it must be sound in both product and process. The process must provide assurances that an individual has been vetted through an identity proofing process. The process should include common criteria and assurances prior to enrollment and token issuance. The more stringent the criteria and assurances are, the higher the level of certainty and trust. Strong criteria may include elements such as background investigations, collection and verification of biometric information, and requirements for presentation of certain identity documents prior to issuance.

[17] Gary R. Gordon and Norman A. Wilcox, *Identity Fraud: A Critical National and Global Threat* (Utica: Utica College, Economic Crime Institute, 2003), 6.

The second prong of the test is the product, or identity token (document, card, or item that is used to establish identity) itself. Trust and certainty are developed through a product that is counterfeit resistant. The ability of the product to resist change and/or duplication develops certainty and trust. The stronger the product is to resist counterfeit, the higher the level of trust and certainty in the answer to the question, "Who is this?"

Process and product come together to form a trust model. Both aspects must be sound to develop certainty. A stringent vetting process backed with a token that can be easily reproduced and altered does not create trust. Likewise an identity token that is strongly resistant to tampering, but was issued without criteria or assurances, also creates uncertainty and is not trusted. Identity authentication is marrying sound process and a tamper resistant product to create certainty and trust.

President Ronald Reagan often quoted the Russian Proverb "Doveryai no Proveryai" which translates to "trust, but verify" to describe his foreign policy dealings with the Soviet Union in the late 1980's.[18] "Trust, but verify" is an appropriate mantra for first responder identity. The solution requires a framework that can provide verification. The infiltration of the response to the TWA Flight 800 disaster evidenced the vulnerability and limitation of trust in the current unverifiable picture/ paper based identity management system. If the TWA disaster had been a terrorist attack, the current system would not have mitigated the threat of secondary attack against first responders.

b. Rapid In-Processing

In-processing for incident response requires that identity and affiliation be verified, the responder be enrolled or logged into the scene, the level of site access determined, and accountability be maintained by tracking personnel on-scene. Rapid in-processing for identity management is the ability to perform these tasks efficiently with minimal impact on the completion of tactical objectives for incident response. The lack of rapid in-processing to incident scenes is documented as a failing of identity management for terrorism incident response. The AAR's for both the Oklahoma City and Pentagon responses indicate that it took hours to provide credentials to personnel for

[18] AP Foreign Desk, "Excerpts from the Reagan Interview with 4 Correspondents," *New York Times*, 4 December 1987.

entry into the scenes. Speed of processing, however, is the competing factor to identity authentication in an incident response setting. Perimeter personnel must weigh security against the immediate need for personnel at an incident scene. Due to the inadequacies of the current identity management system, perimeter personnel are forced to revert to unverifiable credentials and the uniform, emergency vehicle, demeanor consistent with position identity construct. Any identity management solution must provide a level of security and speed that does not hinder, but enhances incident response. The speed of processing should be consistent with the time that would be required for perimeter personnel to check "flash" identification and ask follow-up questions.

c. Interoperability

The Department of Homeland Security SAFECOM program defines interoperability as "the ability of emergency responders to work seamlessly with other systems or products without any special effort."[19] An identity solution for terrorism incident response must have this important capability. The problems of radio interoperability are well documented. They are found among the lessons learned of every AAR and became a central focus of the *9/11 Commission Report*. The same gaps would be found if technology had been broadly applied to identity management for first responders. The implementation of identity management technology for first responders is in its infancy. In its current state, it is the communication equivalent of smoke signals. This can be seen as a problem or an opportunity. Unlike communications, there is not a proliferation of proprietary technology that has been implemented for identity management. This presents an opportunity to promulgate a standards-based interoperable system. Interoperability is a necessary element to enable authentication of responders from varied disciplines and levels of government that converge on incident scenes during the response to acts of terrorism.

d. Data Storage / Retrieval and Promulgation Capability

Data storage / retrieval and promulgation involves the ability to store or link to data in a manner that it can be brought forward for utilization in other processes. An identity management system for improved terrorism incident response must include the capability to store or link data in a manner that can be promulgated to, and utilized by

[19] U.S. Department of Homeland Security SAFECOM Program, "Interoperability," http://www.safecomprogram.gov/SAFECOM/interoperability/default.htm. (accessed 14 July 2006).

incident commanders. Data storage/retrieval and promulgation addresses two aspects deficient in previous response to incidents of terrorism. The first deficit involves the matter of the training credential. The first section of the two part definition of identity was introduced in Chapter I. Section A. It also consists of a second part that includes "the set of behavioral or personal characteristics by which an individual is recognizable as a member of a group."[20]

The group affiliation, or training credential in this case, is essential information for incident commanders to adequately deploy and coordinate appropriate assets to achieve incident objectives. In *Information, Technology, and Coordination: Lessons from the World Trade Center Response*, the importance of information for deployment and coordination of responders is highlighted: "Effective deployment and coordination depend on many kinds of information from the roles and capabilities of response and support organizations to the identity of individual responders."[21] While the effective utilization of assets is a problem of incident management, providing the information concerning the characteristics, group affiliation, or training credential of assets is a function of identity management.

The second deficiency in terrorism incident response that can be addressed through data storage/ retrieval and promulgation is accountability. In the National Commission on Terrorist Attacks upon the United States *Staff Statement No. 14*, the following outlines the deficiency for accountability: "Once units arrived at the WTC they were not accounted for comprehensively and coordinated."[22] Providing this information is a function of a comprehensive identity management system. Would the resources have been uncoordinated and unaccounted had an effective identity management system been in place? A properly structured and effective identity management system would provide real-time usable information to incident commanders concerning the number, location, and qualifications of assets at his/her disposal. Critical to incident commanders concerning personnel resources are the answers to questions such as: "Who is this?", and

[20] *American Heritage Dictionary*, "Identity."

[21] Sharon S. Dawes et. al., *Information, Technology, and Coordination: Lessons from the World Trade Center Response* (Albany: University at Albany, SUNY, Center for Technology in Government, 2004), 9.

[22] National Commission on Terrorist Attacks upon the United States, *Staff Statement No. 14* (Washington, D.C: n.p., n.d.), 8.

"What can they do for me?" An effective identity management system for incident response must provide incident commanders with the data to answer those critical questions.

2. Criteria for Evaluation: Public Policy Considerations

A purely theoretical solution meets the reality of implementation with the consideration of public policy concerns. The utility of a solution lies in its ability to be translated into corrective government action. Policy implementation is predicated on the political acceptability and cost of the program. The incident response criteria described above delineate the utility of the solution relative to the identified problem. The following public policy criteria evaluate the ability of the program to be brought to fruition. Public policy concerns temper the utility to incident response with the capability of the program to be implemented. There is little doubt that any homeland security problem presented can be solved provided it was fully funded and supported with all available resources. The reality is that solutions must be cost effective and politically achievable. Cost is a criterion for consideration in any potential public policy change. This addresses the essential question, "Is the cost of the cure greater than the problem?"

The final element of the criteria for analysis is political acceptability. More than acceptable, the policy must not be unacceptable. In *A Practical Guide for Policy Analysis* political unacceptability is described as "a combination of two things: too much opposition (which may be wide or intense or both) and/or too little support (which may be insufficiently broad or insufficiently intense or both)."[23] The ability to bring the proposed change to fruition is an essential element to the complete analysis of alternatives.

E. SUMMARY

The review of after-action reports of the response to major domestic incidents of terrorism reveals a significant gap in identity management for incident response. Incident response to terrorism is a complex dynamic consisting of many factors. Identity management is an important component of the response and if structured properly can provide not only authenticated identity leading to increased force protection, but

[23] Eugene Bardach, *A Practical Guide to Policy Analysis: The Eightfold Path to Effective Problem Solving* (Washington, D.C.: CQ Press, 2005), 32.

additional information to support scene safety and incident command and control decisions. An effective identity management system that improves incident response must include methods for identity authentication, rapid check-in, interoperability, and capability for data storage/ retrieval and promulgation while considering overall costs and the political acceptability of the solution. The chapters that follow will detail the analysis of three policy options across the six identified criteria. The analysis will reveal a preferred policy option and recommended course of action to close the identity management capability gap for terrorism incident response.

THIS PAGE INTENTIONALLY LEFT BLANK

II. MAINTENANCE OF THE CURRENT DECENTRALIZED IDENTITY MANAGEMENT SYSTEM (OPTION 1)

A. OVERVIEW

The current system of identity management for first responders is completely decentralized and results in extreme differentiation. The process of issuing identity documents or badges to employees and volunteers is not often centralized at a municipal level. It usually rests with each individual municipal agency. There are also countless different issuance criteria that are utilized depending on response discipline, available technology, financial resources, and level of importance placed on identity credentials by the governmental entity. Until recently, the same was true for the federal government and its many agencies and departments. The federal government, under Homeland Security Presidential Directive – 12, has begun the process to consolidate identification into a single federal government identity credential. This system will be further explored as a policy option in Chapter IV.

Identity management systems vary greatly from jurisdiction to jurisdiction. These vast differences make it nearly impossible to trace every possibility for identity solutions that employed throughout the nation. Due to the decentralized nature and extreme differentiation in how identity credentials are handled at the state and local levels, one community will be examined to illustrate and define the scope of the current decentralized system. Frederick County, Maryland will be utilized to examine this system. Frederick County was chosen for three reasons: first, it has an identity management problem that contains many issues relevant to this discussion. Secondly, as there is not an extensive body of knowledge on the problem, Frederick County data was available and access was allowed to information and discussions in much greater detail than was available elsewhere. Third, Frederick County has connections to the National Capital Region which allowed access to the identity project being undertaken that will be described in Chapter IV. Frederick County identity management will be highlighted, and as available data allows, parallels will be drawn between it and other communities across America.

Although the response to incidents of terrorism will involve many levels of government and non-governmental organizations, the study of Frederick County as it relates to the current identity management system will focus on "first responders" as defined in the Homeland Security Act of 2002 and Homeland Security Presidential Directive – 8. The Homeland Security Act of 2002 defines emergency response providers as: "Federal, State, and local emergency public safety, law enforcement, emergency response, emergency medical (including hospital emergency facilities), and related personnel, agencies, and authorities."[24] Homeland Security Presidential Directive – 8 incorporated the previous definition, but expanded on it to include "emergency management, public health, clinical care, public works, and other skilled support personnel (such as equipment operators) that provide immediate support services during prevention, response, and recovery operations."[25] The definition of first responder as applied to Frederick County government entities includes the Department of Fire/Rescue Services, Sheriff's Office, Health Department, Department of Public Works, and one non-governmental organization, Frederick Memorial Hospital. Each of these entities will be explored for identity management processes for the distribution of credentials. Identity authentication is only a portion of the issue, further complicating the matter of credentialing is the interdependencies of systems. Local credentialing is often dependent on state licensure requirements, particularly in the areas of medicine, emergency medical services, and law enforcement. These interrelationships and other issues will be explored and evaluated through the examination of identity credentialing for "first responders" in Frederick County, MD.

B. FIRST RESPONDER IDENTITY MANAGEMENT IN FREDERICK COUNTY, MD

1. Law Enforcement - Frederick County Sheriff's Office

Identity credentialing for law enforcement officers in Frederick County and across the State of Maryland is a cooperative function requiring both state and local action. The certification of police officers is regulated by the Maryland Police and Corrections Training Commission (MPCTC). Under the authority of Section 3-208 (a) of the

[24] Homeland Security Act. U.S. Code Annotated, Vol. 6, Sec. 101(2002).

[25] *Homeland Security Presidential Directive 8: National Preparedness* (Washington, D.C.: The White House, December 2003), 1.

Maryland Public Safety Article the MPCTC regulates the training, background investigation, and criminal history standards for police officer certification. In the process of certifying a police officer, the responsibility of positively establishing identity rests with the local employing agency. The application does not capture verifiable biometric identifiers such as a photograph or fingerprints. Agency verified identity information (Driver's License, Birth Certificate, etc.) is captured on the application for certification and forwarded to MPCTC for review and issuance of a certification document.

The certification document consists only of a paper card with a certificate number, control number, and expiration date. The document does not contain security features, or biometric identifiers. The control and certificate numbers are not verifiable, other than by phone call during normal business hours. The telephone verification does not include biometric or other identifiers, only the status of the card number.

The Sheriff's Office Records Section produces identification for Frederick County Deputies. The identification consists of a digital picture on an adhesive plastic card that is attached on a contactless building access card. The identification does not contain any security features other than a tracking number for the building access card. If lost or stolen the card can be electronically revoked preventing building access. The identity token contains no verifiable information other than the name and employee identification number of the deputy. This information can only be verified by phone call to the agency.

The law enforcement example provided through the Frederick County Sheriff's Office and its relationship to the State of Maryland is similar to many other communities in the United States. Most importantly, Maryland, along with 42 other U.S. States, views police officer certification as a license that requires renewal. It can also be suspended or revoked.[26] In other states, such as Rhode Island, the State sets the minimum standards for suitability and training of entry-level personnel who earn a certificate of completion that cannot be revoked. The system relies upon local employing entities to determine whether an individual is suitable for employment once entry-level requirements are met.

[26] Roger L. Goldman and Steven Puro, "Revocation of Police Officer Certification: A Viable Remedy for Police Officer Misconduct?," *St. Louis University Law Journal* 45, no. 541 (Spring 2001).

This is an important difference that indicates a higher level of 'trust' in the credential of police officers with continuing licensing requirements. Another important element is the absence of nationally recognized and accepted training standards. This further complicates the matter of marrying identity and training levels into a credential. Organizations such as the Commission on Accreditation for Law Enforcement Agencies (CALEA) and The International Association of Director's of Law Enforcement Standards and Training (IADLEST) provide model-based standards for law enforcement policy and administration, however, fall short of prescribing minimum competencies for law enforcement officers.

2. Fire Fighting / Emergency Medical Services - Frederick County Division of Fire/ Rescue Services (DFRS)

Identity credentialing for Fire/EMS personnel in Frederick County, MD is differentiated based on position and paid or volunteer status. DFRS is staffed by only 100 career professional firefighters. The main force, totaling nearly 1300, is made-up of volunteers from independent incorporated volunteer fire companies. The process of identity credentialing is vastly different for professionals and volunteers, as well as differentiated for firefighters and personnel providing emergency medical services.

a. Firefighting Personnel

DFRS firefighting professional staff are subjected to background investigations and fingerprint checks prior to employment. The investigations and checks are completed through the Office of the State Fire Marshal. Once completed, DFRS Fire employees are trained to National Fire Protection Association firefighter II standard before station assignment.[27] Differing from law enforcement, there are options for local jurisdictions in the adoption of training standards. The State of Maryland regulates by law the standards for those personnel who serve as trainers, but does not prescribe content training standards for other personnel. This lack of an enforceable standard results in differences in training and requirements from county to county within the State of Maryland. There are other voluntary compliance options for standardized training through the Maryland Fire Service Professional Qualification Board (MFSPQB). The MFSPQB has prescribed a standardized training curriculum, but its use is voluntary and

27 National Fire Protection Association, *NFPA 1000: Standards for Fire Service Professional Qualifications Accreditation and Certification Systems* (Quincy, MA: NFPA, 2006).

is utilized by only a few agencies across the state. There are also national training standards offered by the aforementioned Nation Fire Protection Association with additional standardized certification also available through the National Board on Fire Service Professional Qualifications.

As independent corporations, the volunteer fire companies are offered the opportunity to have the Office of the State Fire Marshal perform background investigations on prospective members. Very few companies take advantage of this service and accept members without the available checks. As Maryland law does not govern it, the volunteer company determines the requirements and training level. Within Frederick County there is a mix of training levels because of the lack of enforceable state standards.

Both volunteer and professional firefighters are issued plastic identity credential cards. These simple cards contain no security features. The card consists of a digital picture, name of the employee, job function, and name of the organization. These cards are also unverifiable other than by phone call to employing agency or volunteer fire company. They do not contain tracking numbers or other features to maintain accountability.

b. Emergency Medical Services Personnel

The DFRS employees and volunteers of the independent corporations who deliver pre-hospital emergency medical services (EMS) are governed by prescribed Maryland State standards. Maryland Annotated Code Section 13-509 provides the Maryland Institute for Emergency Medical Services Systems (MIEMSS) with the authority to regulate and provide training standards for personnel involved in pre-hospital medical treatment. MIEMSS has adopted regulations consistent with the U.S. Department of Transportation (DOT) National Highway Traffic Safety Administration (NHTSA) standard curriculum for emergency medical services providers.

MIEMSS certification requires specific training and testing to achieve and maintain certification. MIEMSS issues a plastic certification card that contains no verifiable biometric information. The card contains a bar-code and information regarding name and location, level of certification, expiration date, and a certification identification

number that could be verified by MIEMSS during business hours. The State of Maryland, along with 42 other U.S. States, requires Emergency Medical Technicians to meet and maintain the certification standards of the National Registry for Emergency Medical Technicians (NREMT).[28] Unique to the credentialing mechanisms studied thus far, the NREMT maintains an on-line database that may be queried by name and state that provides the current status and level of certification for all registered personnel.

3. Public Health - Frederick County Health Department

Similar to law enforcement, Frederick County Public Health Officials are issued identity credentials through a cooperative state and local process. There is an additional issue as many of the personnel assigned to the Frederick County Health Department are actually employees of the State of Maryland that has a differentiated process. The nurses and physicians employed by either the State or local government are subject to State of Maryland certification requirements for health professionals.

In order practice as a physician or nurse in Maryland, certain qualifications are required to receive and maintain professional licensure. The Maryland Board of Physicians and the Maryland Board of Nursing under the Maryland State Department of Heath and Mental Hygiene determine qualifications. The powers of the boards are codified in the Code of Maryland Regulations Title 10 (Department of Health and Mental Hygiene) Subtitle 29 (Board of Nursing) and Subtitle 32 (Board of Physicians). These sections establish the regulatory authority of the Maryland Board of Physicians and Maryland Board of Nursing for the purposes of licensing professionals. These boards regulate the required initial and continuing education requirements for professional licensure in Maryland. The boards also maintain the authority to suspend or revoke professional credentials for malfeasance and/or failure to meet continuing re-certification requirements.

In order to receive a professional license, the board mandates education and testing requirements. If the requirements are met, a paper credential containing name, certificate type, certificate number, and expiration date is issued. The paper document contains no security features or biometric information. Both the Board of Physicians and

28 National Registry of Emergency Medical Technicians, "About EMS," http://www.nremt.org/about/ems_learn.asp/ (accessed 9 April 2006).

Board of Nursing maintain searchable on-line databases. This allows for internet confirmation of license status. The database is searchable by name or certificate number anytime. Due to the open nature of the search function no identifying information other than name, practice address, and status are shown as search results.

The physicians and nurses employed by the Frederick County Health Department are required to maintain professional certification. Both state and county employees are issued Frederick County identification cards. These are simple plastic cards that contain basic information, photo, and no security features or accountability process. The employment process for Frederick County personnel does not include background checks beyond the verification of professional license and routine pre-employment practices. In contrast, employees of the State of Maryland are subject to additional fingerprint and criminal background checks before employment. The State employees are then issued an additional identity credential that contains a photo and information concerning job function, and certification.

A recent program developed by the U.S. Department of Health and Human Services is seeking to provide personnel definitions and credentialing in healthcare nationwide. The Emergency System for Advance Registration of Volunteer Health Professionals (ESAR-VHP) Program seeks to "develop a system that allows for the advance registration and credentialing of clinicians needed to augment a hospital or other medical facility to meet increased patient/victim care and increased surge capacity needs."[29] The desired outcome of the program is "...all States will have an ESAR-VHP System developed in coordination with HRSA's ESAR-VHP program, allowing for a national system of mutual assistance of health volunteers within a State's public health structures and hospital systems."[30] The ESAR-VHP definitions provide leveled emergency credentialing standards for physicians, registered nurses, marriage and family therapists, medical and public health social workers, mental health and substance abuse

[29] U.S. Department of Health and Human Services, Health Resources and Services Administration, *Emergency System for Advance Registration of Volunteer Health Professionals Program: Interim Technical and Policy Guidelines, Standards and Definitions* (Washington, D.C.: HRSA, 2005), 3.

[30] Ibid, 17.

social workers, psychologists, mental health counselors, and behavioral health professionals. The program is advancing with a target date of December 2006 for state implementation.

4. Clinical Care - Frederick Memorial Hospital

Clinical care and public health realms are governed by the same overarching structure. The clinical care staff of Frederick Memorial Hospital are governed by the same State of Maryland regulations and professional standards boards as the public health professionals. The physicians and nurses employed by Frederick Memorial Hospital are subject to additional checks by the hospital before privileges are granted. After hiring, personnel are provided with plastic access badges that contain digital photograph, job assignment and contain magnetic stripe technology that is integrated with hospital access control systems. The plastic badges issued to personnel serve to allow access to restricted areas of the hospital through magnetic stripe technology that allows access based on entry requirements. As the ESAR VHP program advances in Maryland, clinical care staff that choose to volunteer can register through the program to have established emergency credentials.

5. Public Works - Frederick County Division of Public Works

The Frederick County Division of Public Works has the most diversified workforce of the County Agencies. Public Works operations include a wide spectrum of employees from professional engineers to highway operations equipment operators. Many of the positions require professional licensure under the Code of Maryland Regulations Title 9 Department of Labor, Licensing, and Regulation. For example, many employees of the Division of Public Works require licensure from several boards under this title including the Board of Architects, Board of Master Electricians, Board of Examining Engineers, and Board of Plumbing. Although the professional positions are regulated by board requirements, many of the other positions are not governed by overarching standards, outside of commercial driver's license requirements, including highway operations and heavy equipment operators, who receive only on the job training. Both professional and operations staff are issued plastic identity cards after standard pre-employment screening that does not include fingerprint or background investigations. The card contains a picture, name, job title, and no inherent security features.

The Public Works credentialing situation in Frederick County is similar to other areas of the country. In the January, 2005 edition of the American Public Works Association Magazine, *Reporter*, author Larry Lux describes the problem for public works nationally.

> Perhaps our weakest area is in the qualifications and certifications of our personnel. While our emergency personnel are generally expertly prepared and well trained for their day-to-day jobs, unlike our colleagues in other disciplines… we do not have a peer review process that issues credentials certifying the competencies and training of public works professionals. [31]

Public Works as a discipline presents the greatest challenge. Oversight and standards for other disciplines vary, but they are assisted by existing national standards, and/or state regulations, that govern their training and certification.

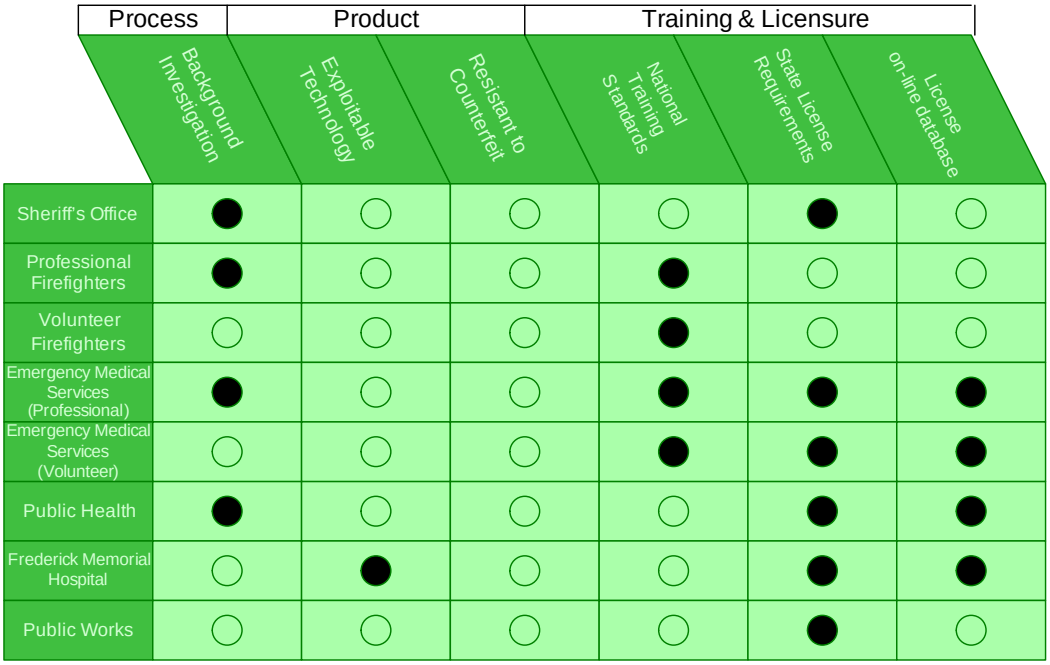

Table 1. Summary: Identity Management in Frederick County First Response Agencies

[31] Larry Lux, "The impact of Homeland Security Presidential Directive 5 on the public works community," *American Public Works Association Reporter Online*, (January 2005), http://www.apwa.net/Publications/Reporter/ReporterOnline/index.asp?DISPLAY=ISSUE&ISSUE_DATE=012005&ARTICLE_NUMBER=960/ (accessed 14 May 2006).

C. EVALUATION

The previous sections detail the current status of first responder identity as it relates to the disciplines of law enforcement, firefighting, emergency medical services, public health, clinical care, and public works. The current system will be evaluated utilizing the criteria developed in Chapter I Part C Section 2 of this thesis which include identity authentication, rapid in-processing, interoperability, data storage/ promulgation capability, cost, and political acceptability. The criteria were identified as the elements necessary in a credential for the successful response to an incident of terrorism.

The current system, as identified through the example of Frederick County, MD, provides no ability for identity authentication. The heart of identity authentication is trust model identified previously as the ability to "trust, but verify". The documents that would be presented in the response to an incident of terrorism in Frederick County and most of America are unverifiable, lack security features, and lack an issuance process that develops trust. The process of identification issuance at the Frederick County Sheriff's Office is the closest to providing a trusted identity, as the extensive nature of the background investigation and hiring process provides a level of certainty as to the identity of the individual. The trust developed in a sound process is then diminished through the issuance of an easily counterfeited unverifiable paper identity token. The current first responder identity credentials in Frederick County do not provide methods for the authentication of identity.

The evaluative criteria rapid in-processing is also deficient in the current identity system for first responders. In our example community, the credentials issued to Frederick County government personnel do not allow for rapid in-processing in the event of an incident. In addition to no security features, the identity tokens also do not contain any exploitable technology features (bar-code, magnetic strip, etc.) that would enhance in processing capability. If the technology were present, there is currently no available resource to manage on-scene identity or equipment to exploit the technology. The current status would require complete in-processing and issuance of an incident specific identity. The current state of first responder identity does not allow for rapid in-processing.

The evaluative criteria for interoperability and data storage/promulgation capabilities are related as they both require a technological solution. As the credentials issued in Frederick County and many other jurisdictions across the nation do not contain exploitable technological features, they lack the capability for interoperability and data storage/ promulgation. In addition, credentials issued are in most cases created and issued without jurisdictional system design. Each of the agencies in Frederick County utilizes different tokens and issuance processes. There is no common standard or as previously described, exploitable technology feature. The identity tokens are not interoperable nor do they have the capability to store or transfer data.

The evaluative criteria cost is what continues to keep the current decentralized identity system as an attractive option. Cost data was not available for each of the agencies or Frederick County as a whole; however, the low cost of unverifiable no-tech identity cards is what drives their proliferation. These cards cost only a few cents each, and they provide the community a solution equal to their perceived level of risk. In most cases, the higher the perceived risk or need for security in a community, the better technology the community will employ. The current identity system meets the day to day needs of most organizations, but will fail under stress.

Most communities are not willing to make the significant investment required to overhaul identity management systems to provide the benefits to low probability events such as incidents of terrorism. The compelling argument for utilizing technologically advanced systems is the integration of e-government initiatives. E-government is defined by the Center for Technology in Government Report *Making a Case for Local E-Government* as "the use of information technology to support government operations, engage citizens, and provide government services."[32] Examples of the benefits of e-government initiatives cited by the report include increasing efficiency by streamlining business processes, improving internal communication, providing better customer

[32] Meghan Cook et al., *Making a Case for Local E-Government* (Albany: SUNY University at Albany, Center for Technology in Government, 2002), 3.

service, keeping up with citizen demands and expectations, and promoting what local governments do well. [33] The increased investment in identity related technology must translate into public value.

The current system creates little in the way of public value as it does not provide benefits to other government processes or address essential functions in the response to terrorism. In turn, this system costs little, justifying its existence. Viable alternatives must create public value by providing benefits and cost savings to other government ventures. The low cost of the current system makes it attractive as a continuing option. The issue of cost is also intertwined with political acceptability as it relates to the development of minimum basic competencies that form the training aspect of a credential.

The current decentralized system is politically acceptable to state and municipal governments as it has developed under the Constitutional principle of federalism, and until recently absent the threat of terrorism. The Tenth Amendment of the United States Constitution states, "The powers not delegated to the United States by the Constitution, nor prohibited by it to the states are reserved to the states respectively, or to the people."[34] The current decentralized identity system is aligned with the federal system of dividing power between levels of government embodied in the United States Constitution. The power to prescribe the qualifications and training for professions are within the regulatory 'police powers' of the State. Police powers are described in the Supreme Court Case U.S. v. E.C. Knight Co.: "It cannot be denied that the power of the state to protect the lives, health and property of its citizens and to preserve good order and the public morals, the power to govern men and things within the limits of its dominion, is a power originally and always belonging to the state, not surrendered to the general [federal] Government, nor directly restrained by the Constitution of the United States, and essentially exclusive."[35] The power to prescribe general qualification definitions and methods for the issuance of identity documents are inherent to the duties reserved to the States by the United States Constitution. The current system is politically

[33] Cook et al., *Making a Case for Local E-Government*, 4-5.

[34] United States Const., Amend. X.

[35] *United States v. E.C. Knight Co.*, 156 U.S. 1 (S.Ct. 294 1895).

acceptable as it is consistent with current practices and authorities. Political acceptability is not necessarily a positive characteristic as it relates to the improvement of identity management for terrorism incident response. It is, however, a necessary element to consider in the implementation of proposed solutions. The legalities and relationship between the powers of the state and federal governments established by the United States Constitution and relevant case law are essential considerations in implementation strategies. The current system has developed under Constitutional delegated authorities absent the eventuality of terrorism.

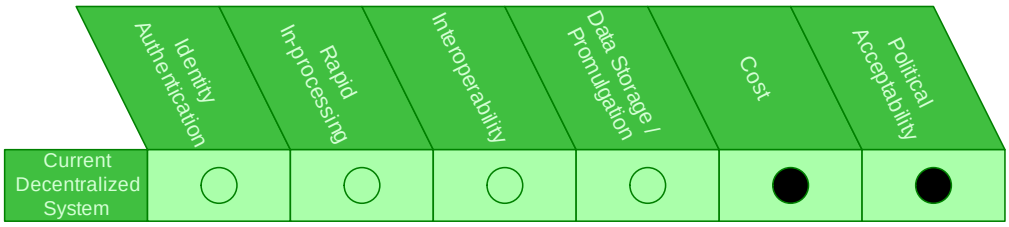

Table 2. Evaluation Matrix: Decentralized Identity Management System

D. SUMMARY

The current decentralized identity management system for first responders is fragmented at best. The snapshot of one community showed the disparity in the methodology for the issuance of identity credentials across disciplines and the complexities governing the regulation of professional and training credentials. The current system is a puzzle that does not develop trust and returns little to the public. Trust in an identity system is predicated on marrying strong product and process. As demonstrated in the Frederick County example, there is disparity in process and product within just one jurisdiction. When multiplying that effect across the American federal system, the result is the possibility of thousands of processes and products resulting in a critical identity trust gap. The current State of identity management provides almost no larger benefit to the response to incidents of terrorism. The *National Incident Management System* (NIMS) identifies that "credentialing involves providing documentation that can authenticate and verify the certification and identity of designated

incident managers and emergency responders."[36] The current identity system does not provide the mechanism to credential across disciplines for improved terrorism incident response.

Arguably, as with many areas of government, the current system was not designed for the eventuality of terrorism. When considered absent of the threat of terrorism the system also does not provide public value equal to its potential benefit. It is obvious the current credentialing system was developed with no overarching design. The regulation among the disparate disciplines have come together under the moniker of first responders, exposing stark differences and definitional problems as it relates to processes for secure identity and the need for basic training competencies. A shift in the paradigm for first responder credentialing is essential for improved terrorism incident response.

As identified through the evaluation of the identified criteria, the current system provides no inherent factors that support improved response to incidents of terrorism. The current identity system satisfies traditional concerns over cost and acceptability to the political system; however, it provides little public value or benefit to the overall delivery of government services. The challenge in identity management for improved terrorism incident response is to create a framework that leverages existing investments to increase public value. An improved identity management system that provides benefits, not only to terrorism response, but improves processes and results in greater efficiency in the delivery of public services is a necessary. The current system as outlined is a hindrance to the delivery of timely assistance in the event of a catastrophe that requires a large multi-jurisdictional government response.

[36] U.S. Department of Homeland Security, *National Incident Management System* (Washington, D.C.: GPO, 2004), 46.

III. IDENTITY MANAGEMENT TEAMS FOR TERRORISM INCIDENT RESPONSE (OPTION 2)

A. OVERVIEW

The concept of identity management teams for incident response is not novel. A version of this solution has been implemented at every major incident of terrorism out of necessity. The need to control access and positively identify personnel on terrorism incident scenes was recognized with our first domestic attack on the World Trade Center in 1993. The impetus in 1993 was the need to control access to the crime scene.[37] The additional threat of secondary attack as described in Chapter I of this thesis shows increased urgency for effective incident scene control and credentialing. The failings of identity credentialing during the 1995 Oklahoma City Murrah Federal Building bombing, and the 2001 responses to the World Trade Center and the Pentagon were pervasive and discussed in Chapter I Section 1. The Arlington County and Oklahoma City After-Action Reports are instructive, however, as the failings of identity management early in the incident were tempered with later success. The systems that were instituted over the course of the incidents, through trial and error, provide best practices and a concept of operations at the heart of what should comprise an on-scene identity management team for terrorism incident response.

As established through the analysis of historical responses to incidents of terrorism conducted in Chapter I, identity management is a major deficiency for terrorism incident response. Despite this deficiency, there is currently not a defined response asset under the FEMA National Mutual Aid and Resource Management Initiative to address this important function. The National Mutual Aid Resource Management Initiative "supports the National Incident Management System by establishing a comprehensive, integrated, national mutual aid and resource management system that provides the basis to type, order, and track all (Federal, State, and local) response assets."[38] The resource definitions are typed so the level of capability of resources can be readily determined

37 Federal Emergency Management Agency, United States Fire Administration, *The World Trade Center Bombing: Report and Analysis* (Emmitsburg, MD: USFA, 1993), 135.

38 U.S. Department of Homeland Security, Federal Emergency Management Agency, *Typed Resource Definitions: Law Enforcement and Security Resources* (Washington, D.C.: FEMA, 2005), 2.

before an asset is requested. The problem is that there is no resource definition that performs the function of identity management for incident response. Currently, if an incident commander needed assistance in managing access to the scene through a credentialing system, there are no typed assets to order through mutual aid or other process to perform this function, leaving a glaring capability gap.

The Frederick County Sheriff's Office, in recognition of the law enforcement responsibility for force protection, scene control, and crime scene protection in the event of a terrorist incident, developed a proposal to the State of Maryland for a demonstration project to overcome the identity deficiencies of first response agencies in Frederick County described in detail in Chapter II. The proposal seeks the development of an operational typed response resource to perform identity management functions on the scene of a terrorist incident. The intent of this chapter is twofold: first, to explain the rationale for the resource definition as developed for the proposed demonstration project and second, to evaluate the product across the defined response and public policy criteria to determine its suitability to close the identity management capability gap for terrorism incident response.

B. IDENTITY MANAGEMENT TEAM CASE STUDIES

The explanation of the rationale begins with the examination of the 1995 Oklahoma City Murrah Federal Building bombing and the 9/11/01 Response to the Pentagon to clarify the development of the resource definition and typing for the proposed identity management response resource. These incidents and after-action reports provide significant detail regarding the development of ad-hoc identity management capabilities as the incidents unfolded. Parallels will be drawn utilizing other published documents that highlight, but do not provide enough significant detail for case study. The review of these incidents reveals a baseline structure for a typed identity management resource. The resource definition as developed by the Frederick County Sheriff's Office will be analyzed across the identified criteria for public policy considerations and improved terrorism incident response as it relates to closing the identity management gap for terrorism incident response.

1. 1995 Oklahoma City Murrah Federal Building Bombing

In the response to the 1995 Oklahoma City bombing incident many lessons were learned concerning the structure, function, concept of operations, importance of site access control, and the need for dedicated identity management resources. The Oklahoma City incident provides the background for the first large-scale terrorist incident that required a robust capability for identity management and scene control. Through trial and error, and utilizing only available resources, an ad-hoc identity management capability was developed and sustained that allowed for the issuance of over 28,000 identity credentials over the course of the incident.

The initial failure of identity management at the incident scene was the lack of any pre-planned credentialing option. This lesson learned is captured in the recommendations of the After-Action Report. Although the capability gap is clearly identified in the report, eleven years later there still remains no guidance, or nationally defined resource to perform this critical function. This subsection seeks to close the gap first exposed in the Oklahoma City response by defining a response asset for this critical function.

The development of on-scene identity credentialing first requires the establishment of a perimeter. In the case of the Oklahoma City bombing, establishing a controlled perimeter around the incident site occurred within two hours of the blast.[39] Once the perimeter was established the Oklahoma City Police Department (OCPD) utilized its only available asset to issue identification by moving its Permit and Identification Section equipment to the scene to issue identification badges. The Permit and Identification Section was not a deployable asset; however, it was the only available option for credentialing. Once established, the operations of the Permits and Identification Section lasted only a few hours as identity supplies were quickly exhausted.[40]

The OCPD continued to issue alternative forms of identification: "different colored passes were issued for each day after April 20th to discourage people from

[39] City of Oklahoma City, *Alfred P. Murrah Federal Building Bombing April 19, 1995: Final Report*, 369.

[40] Ibid, 39.

returning to the site when they had no current assignment."[41] Due to rain and lighting conditions, the location of the identity station changed three times. When agents from the Federal Bureau of Investigation (FBI) arrived, they also began issuing identification, causing confusion for those manning the perimeter. FBI and OCPD finally consolidated their operations and issued one form of identification, operating from a vacant warehouse building. This is informative for the concept of operation for the employment of an identity management resource, as it must be integrated and maintain a permanent location throughout the incident.

In *Oklahoma City – Seven Years Later: Lessons Learned for Other Communities*, it is reported that early in the response "the ID process was a major issue due to lack of controls and systems in place. No one had been designated to issue ID's and the system was hit and miss."[42] This is instructive in defining an identity asset as it must include controls and systems, and be specifically designated to perform the function with a direct link to on-scene unified command.

The After-Action Report also details the process utilized for credentialing volunteers and rescue workers.

> The process was as follows: volunteers appeared at the Permits and ID location and filled out a permit form with their name, agency, and destination. This permit form was submitted along with a photo ID. The Investigator would inquire as to reasons for accessing the scene. The permit would be approved or denied based on the reason and destination. The Investigator entered the information into a logbook, signed the permit, and sent the volunteer to the FBI photo section for their photo ID. If there were questions about the admittance of a person, the FBI made the final determination.[43]

The excerpt from the After-Action Report gives detail to the process for issuing on-scene identity credential documents. It included examination of identity documents, affiliation and destination, collection of a photograph, and recordation of the issued document.

---

[41] City of Oklahoma City, *Alfred P. Murrah Federal Building Bombing April 19, 1995: Final Report*, C-217.

[42] Oklahoma City National Memorial Institute for the Prevention of Terrorism, *Oklahoma City- Seven Years Later: Lessons Learned for Other Communities*, 11.

[43] City of Oklahoma City, *Alfred P. Murrah Federal Building Bombing April 19, 1995: Final Report*, C-217.

These elements form the basis of a minimum inspection necessary for entrance to a terrorism incident scene. Another essential element of the identity management function is communications equipment. Credentialing staff utilized "a cellular phone and a police radio….when trying to check on whether a volunteer should gain access to the scene."[44] Communications equipment and the aforementioned direct contact with on-scene incident command are essential elements in a response asset for identity management.

The process was not without criticism. The After-Action Report details that, "Due to the number of persons requesting entry, the limited resources for processing permits, and lack of guidelines, this process generated complaints. Complaints came from rescue workers and volunteers about the length of time to obtain a permit and the restrictions on the permit."[45] The identity process undertaken during the Murrah Federal building bomb response was completed by hand, not utilizing computerized processes. The After Action report advises "The entire process would probably have gone more smoothly had investigators been able to utilize lap top computers to enter the necessary data on the volunteers."[46] The defined response resource must include computerized processes that allow data and biometric information to be quickly captured and stored to allow access at later times to facilitate processing for re-entry into the scene.

The Oklahoma City Murrah Federal Building bombing response provides baseline information on the development of a defined resource to improve identity management for terrorism incident response. Based on the lessons learned from the response, seven elements for the concept of operations and necessary equipment for an identity management asset for incident response are revealed. The elements related to the concept of operations of a defined resource include a pre-planned solution, an established perimeter, a defined location for distribution, systems and controls including a defined issuance processes and tracking of issued credentials. The lessons learned also revealed necessary equipment and identity supplies including mechanisms to receive replenishment, communications equipment (interoperable radios, internet, and database

[44] City of Oklahoma City, *Alfred P. Murrah Federal Building Bombing April 19, 1995: Final Report,* C-217.

[45] Ibid.

[46] Ibid.

access), computer equipment for identity document production (digital cameras, computers, identification printers). The lessons learned and ad hoc developments during the response to the Oklahoma City Murrah Federal Building bombing form the basis of a defined resource for identity management for incident response.

2. 9/11/01 Pentagon Response

The response to the terrorist attack on the Pentagon on 9/11/01 also revealed many lessons learned concerning the structure, function, concept of operations, importance of site access control, and the need for dedicated identity management resources. The Pentagon attack provides additional background for large-scale terrorist incident response that required a robust capability for identity management and scene control. As with the Oklahoma City Murrah Federal building bombing, credentialing at the Pentagon also developed through trial and error, utilizing available resources. The Pentagon response also tested the boundaries of a limited credentialing solution developed by the Arlington County Police Department in the wake of the identity failures in the Oklahoma City Murrah Federal building response. The development of the credentialing function at the Pentagon incident site is also instructive as its evolution informs the development of a resource definition for an identity management team for improved terrorism incident response.

Understanding the lessons learned from the 1995 Oklahoma City bombing, the Arlington County Police Department pre-planned an identification system for incident scene security and accountability. The system consisted of 2,000 red, yellow, blue, and green colored wristbands to be used for entry to an incident scene. In the tremendous public safety response to the terrorist attack at the Pentagon, Arlington County deployed its identity management system two days into the response. Once the system was utilized, the wristband supply was exhausted within two hours.[47] This failure is instructive in that it took two days to implement an access control system and that identity supplies must be significant to support issuance to thousands of responders. This critical failure further

[47] Titan Systems Corporation, *Arlington County: After Action Report on the Response to the September 11 Terrorist Attack at the Pentagon*, C-23.

enhances the argument for a defined deployable identity management resource staffed by trained personnel that possess the appropriate equipment and supplies is essential for improved terrorism incident response.

On the third day of the response, the Defense Protective Service (DPS), similar to the tactic employed by Oklahoma City Police in 1995, utilized its available badging equipment to produce identity credentials. The DPS system is described in the After-Action Report as "burdensome"[48] and "inadequate for a task of this magnitude."[49] In addition it is described that the badging process "took too long, delaying shift changes inordinately."[50] The AAR also describes "because of the limited computers to create badges and lack of a single database, processing added an additional burden to crew relief."[51] This is instructive in that a defined identity management resource must have adequate computer stations and utilize a single database. This also further evidences the need for a defined as asset as ad-hoc solutions have wasted valuable time as lessons are learned in identity management for incident response time and again at the cost of safety, force protection, and lost on-scene work hours.

At the request of DPS and the FBI, the identity system was bolstered by the addition of United States Secret Service (USSS) identity assets. The AAR describes that the USSS trained members of the Army Band to operate its five portable badge-making workstations.[52] After the incorporation of the USSS equipment the system was described as "effective."[53] The addition of more appropriate equipment and trained personnel resulted in system that was more effective. This is instructive in the development of a defined resource as the number of workstations must permit sufficient throughput not to hamper on-scene operations.

The 9/11/01 Pentagon response provides further validation to the baseline information provided by the study of the Oklahoma City Murrah Federal building

[48] Titan Systems Corporation, *Arlington County: After Action Report on the Response to the September 11 Terrorist Attack at the Pentagon*, A-69.

[49] Ibid.

[50] Ibid., C-58.

[51] Ibid., A-69.

[52] Ibid., C-23.

[53] Ibid.

bombing for the development of a defined resource to improve identity management for terrorism incident response. In addition to the lessons learned from the response to Oklahoma City incident, the Pentagon response provides additional information for the construction of a defined identity management resource. Lessons learned indicate the need for adequate supplies, sufficient workstations to provide reasonable throughput, and the need for a central database. These additional factors when combined with the elements revealed in the response to the Oklahoma City incident develop the baseline of a defined resource for identity management functions on incident scenes.

C. IDENTITIY MANAGEMENT TEAM: TYPED RESOURCE

The lessons learned and basic necessary elements of an identity management team were revealed through examination of the 1995 Oklahoma City Murrah Federal building bombing and the 9/11/01 response to the Pentagon. The elements related to the concept of operations of a defined asset include a pre-planned solution, an established perimeter, defined distribution location, a direct link to on-scene incident command, systems and controls including a consistent issuance processes and tracking of issued credentials. The lessons learned also revealed necessary equipment, including: a significant amount of identity supplies and mechanisms to acquire additional materials, communications equipment (interoperable radios, internet, and database access), computer equipment sufficient for significant throughput for identity document production (digital cameras, computers, identification printers), and a single centralized database. Utilizing these lessons learned and basic elements, the following resource definition was developed. The Identity Management Team (IDMT) resource as defined below was developed by the Frederick County Sheriff's Office and considered by the State of Maryland for the purposes the 2005 statewide resource inventory program.

RESOURCE:	IDENTITY MANAGEMENT TEAM (IDMT)					
CATEGORY:	Law Enforcement/Security			KIND:	Team	
MINIMUM CAPABILITIES:		TYPE I	TYPE II	TYPE III	TYPE IV	OTHER
COMPONENT	METRIC					
Equipment	Computer Equipment	5 Identity Issuance Stations (5 Computers, 5 Digital Cameras, 5 ID Printers, Multi-Technology Readers)	3 Identity Issuance Stations (3 Computers, 3 Digital Cameras, 3 ID Printers, Multi-Technology Readers)			
Equipment	Communications	Team Radio Communication Equipment (portable radios, extra batteries, battery charger, cellular phones)	Team Radio Communication Equipment (portable radios, extra batteries, battery charger, cellular phones)			
Equipment	Communications	Wireless Internet Access, external LE database access	Wireless Internet Access, external LE database access			
Equipment	Software	Database accessible by Incident Command	Database accessible by Incident Command			
Equipment	Computer Equipment	Hand-held remote verification capability	Hand-held remote verification capability			
Equipment	Identity Supplies	10,000 interoperable Identity Tokens Extra printer cartridges Mechanism to obtain additional supplies	5,000 interoperable Identity Tokens Extra printer cartridges Mechanism to obtain additional supplies			
Equipment	Generator	Able to work at location without land line electricity	Able to work at location without land line electricity			
Personnel	Training	Team Trained to Operate Equipment and perform identity functions	Team Trained to Operate Equipment and perform identity functions			
Personnel		1 Officer in Charge (OIC) 1 Supervisor 6 Officers	1 Supervisor or OIC 4 Officers			
Vehicles		Integrated in mobile asset or deployable to a fixed location	Integrated in Mobile Asset / or deployable to fixed location			
COMMENTS:	Type I – A predesignated team consisting of 1 OIC, 1 Supervisor and 6 Officers in an integrated mobile response asset. The team has the ability to manage identity management functions for large-scale incidents. The team engages in routine training to maintain advanced skill level. Type II – A predesignated team consisting of 1 Supervisor or OIC and 4 Officers in an integrated or deployable to a fixed location. The team has the ability to manage identity functions for small to mid-sized events. Team engages in routine training to maintain advanced skill level.					

Table 3. Identity Management Team Resource Definition

The function of the IDMT is to provide identity authentication and accountability support to incident command through the implementation of a comprehensive on-scene credentialing system. The IDMT function is dependent upon the establishment of a strong perimeter as evidenced by the analysis of the Oklahoma City and Pentagon Incidents. The concept of operations also must include deferment of un-requested assets to a secondary staging area. The FEMA report *Responding to Incidents of National Consequence: Recommendations for America's Fire and Emergency Services Based on The Events of September 11, 2001, and Other Similar Incidents* recommends "There should be a separate marshalling area at the incident base for unrequested/ unverified resources. This 'corral' concept was used in Oklahoma City. For added security, law enforcement should manage the perimeter of these areas."[54] This recommendation is incorporated into the IDMT concept of operations outlined in Figure 1.

The study of the Oklahoma City Murrah Federal Building bombing and the Pentagon attack also revealed the need for a consistent system of identity issuance. The Oklahoma City AAR detailed the process that was utilized to issue credentials, however, the Pentagon AAR does not provide sufficient detail that describes the mechanisms of the issuance process. The paper based system that was developed out of necessity and availability of materials can be greatly enhanced with the advent of readily available technologies that can populate data into software from existing identity credentials, such as readers for 2D barcodes or magnetic stripes that have been incorporated into many state drivers' licenses. In addition, the necessity to maintain connectivity to law enforcement and other databases allows for further inspection of identity as outlined in the resource definition (Table 3). This allows for verification of identity through other sources should inspection and electronic implementation of available credentials require addition investigation.

Utilizing exploitable features of existing identity credentials coupled with agency issued credentials can greatly enhance the ability to examine documents and rapidly populate data into a database for a smooth and rapid process for credential issuance. In

[54] Federal Emergency Management Agency, United States Fire Administration, *Responding to Incidents to National Consequence: Recommendations for America's Fire and Emergency Services Based on the Events of September 11, 2001, and Other Similar Incidents* (Washington, D.C.: FEMA, 2004), 50.

some jurisdictions it may also be possible to pre-populate the database with responder information/ biometrics that can be utilized in emergency response situations requiring tight scene controls. Individual jurisdictions or regions may choose to issue responder credentials with exploitable technology that can further improve the on-scene credentialing process.

The Department of Defense program Defense Cross Credentialing Identification System (DCCIS) has developed a web-base option for identity verification for non-government personnel requiring access to government resources.[55] The Federation for Identity and Cross-Credentialing Systems (FiXS) maintains the ability to authenticate identity through the maintenance of a system that allows companies to keep their employee data in their own system that is only accessed when a credential is presented for authentication. The structure of the system alleviates privacy concerns as data is not maintained in a single accessible database. This model is not a strong option for applicability to identity for incident response as communications have traditionally failed in response to incidents of terrorism. The dependence on a web based system would require assurances of continued access through the evolution of an event. This is not a dependable option based on previous response experience.

The implementation of an interoperable or technology based solution at the local or State level will continue to require a dedicated resource to manage identity. A technological solution does not eliminate the need for the function to be managed and maintained on-scene. In addition, not all responders will be issued the same credential, particularly across private-sector agencies that are critical to the success of response and recovery operations. Those not issued credentials pre-event will require the on-scene identity issuance capability of a defined Identity Management Team.

[55] *Federation for Identity and Cross Credentialing Systems*, "Welcome to FiXS," http://www.fixs.org/ (accessed 9 June 2006).

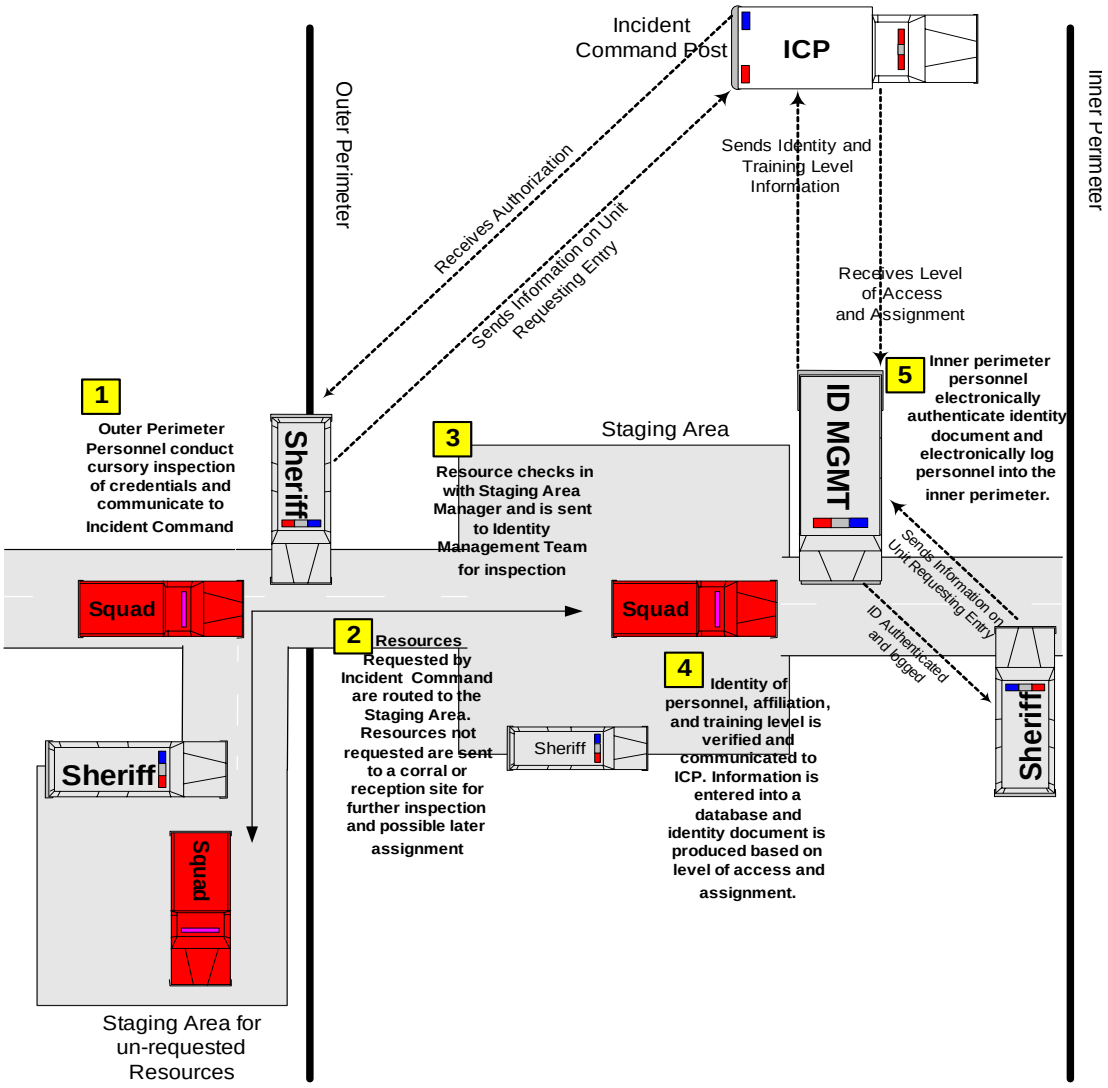

Figure 1. Identity Management Team Concept of Operations

D. EVALUATION

The Identity Management Team (IDMT) resource as defined above incorporates the identity management lessons learned and best practices of the response to the 1995 Oklahoma City Murrah Federal Building bombing and the 2001 response to the Pentagon attack. The IDMT as a defined resource will be evaluated utilizing the developed criteria. The incident response criteria as developed in Chapter I include identity authentication, rapid in-processing, interoperability, and data storage/ promulgation. The additional public policy criteria include cost and political acceptability. The Identity Management Team as defined at the type one level will be evaluated utilizing the criteria.

The first evaluative criterion is identity authentication. The Identity Management Team (IDMT) does not address the endemic first responder credentialing problem of identity authentication, nor does it develop a pre-event system-wide trust model. The resource definition does provide the mechanism to institute an on-scene trust model that can authenticate identity utilizing disparate credentials, evidenced by the examination of Frederick County, MD in Chapter II. The resource as defined does provide the capability to authenticate identity through exploitation of technological options included in other forms of identity. Additionally, the connectivity capability required by the resource definition provides the ability to conduct additional inspection of individuals through database access. Connectivity and ability to access motor vehicle information, criminal histories, etc. provides the mechanism to perform on-scene identity authentication. Although the circumstances of incident response may make connectivity impossible, the exploitation of data encoded through other sources such as state motor vehicle authorities does provide an additional level of certainty.

The rapid in-processing criterion is developed from the analysis of the historical responses to terrorism in Chapter I. The AAR documents from both incidents detail the need for credentialing, but also identify its shortcomings in the responses because of the inordinate length of time for the identity issuance process. The IDMT will serve to reduce this time through the implementation of a pre-planned, pre-designated resource with trained personnel to perform credentialing functions. If this resource were developed in our example community from Chapter II, it would reduce, but not solve the problems associated with credentialing delays. The pre-training and pre-designation would speed the on scene lessons learned of implementing ad-hoc systems as was required in the response to both case study incidents. The Frederick County example shows there is a lack of cohesiveness in the issuance process or the token utilized for first responder identity documents. The IDMT would most effectively function in a pre-planned system where most of the first responders were pre-credentialed utilizing any number of technological options, from inexpensive bar-codes or magnetic strips to more expensive RFID (Radio Frequency Identifier) and smart card technologies. Exploitable technologies and consistency in identity tokens are the key to rapid in-processing.

The IDMT as defined also does not directly address interoperability as a systemic problem for the issuance of pre-event/ daily use professional identity credentials. The IDMT does address on-scene identity interoperability through a preplanned identity system that relies on technological solutions to many of the identity shortfalls outlined in previous incident response. Although the resource definition does not specify the technology option (barcodes, biometric, smart cards, etc.), it does outline the need for technology options that can be read and recorded by handheld devices or remote stations. This requirement achieves on-scene interoperability through the ability to electronically verify issued credentials against the incident database that contains authorizations regardless of the technology option employed. Further research and evaluation through exercise should be conducted into specific technologies to perform this function. Prescribing a technological option at this time, without testing and evaluation, would be presumptive. As defined, an IDMT does account for on-scene interoperability through a common on-scene credential achieving interoperability regardless of the specific technology employed.

The criterion for data storage/ promulgation is developed out of the need to connect identity and level of training for incident commanders to efficiently and appropriately utilize personnel to achieve tactical objectives on incident scenes. For the example community in Chapter II, the IDMT would capture the data through the enrollment process and utilize a centralized database to link the identity token to the individual. Information concerning level of training and identity would be entered into the database during enrollment to connect identity and level of training and be made available to incident command. Depending upon the technological solution employed, the information would be stored in a central database or for more advance technologies stored directly on the token (smart cards). As exposed during the evaluation of other identified criteria, the IDMT does not provide a systemic pre-event solution to the problem of data storage/ promulgation, but seeks to achieve the operational capability on the incident scene. This represents a significant improvement over the ad-hoc solutions implemented at the described incident scenes, but does not provide a complete pre-event solution to the problem.

The cost criterion is developed from traditional public policy concerns. This forces the problem and potential solutions to be judged in the context of the cost to solve the complication, verses the potential total cost of the underlying problem if left unsolved. As the defined resource has not been developed and tested, a total cost has not been previously recorded. The Frederick County, MD Sheriff's Office developed cost estimates for the demonstration project funding proposal to the State of Maryland for a Type II Identity Management Team in an existing mobile asset. The preliminary estimate for cost was approximately $140,000, which did not include the cost of acquiring the trailer.[56] The estimate was developed utilizing low cost bar code technology for on-scene identity issuance, but maintaining the capability to read and authenticate smart card technology. The estimate represents the extreme minimum for the development of an IDMT resource.

Cost and political acceptability are often intertwined. The ability to bring the proposed change to fruition is essential. The development of an IDMT is not extremely cost prohibitive, therefore, it does not affect its ability to be politically acceptable. In the context of the development of an IDMT, there are no legal or political impediments to the development of IDMTs for incident response. The Federal Emergency Management Agency has already defined 120 response resources through the National Mutual Aid and Resource Management Initiative.[57] These definitions have been accepted for intra and interstate mutual resource requests and have not resulted in strong political opposition from the states. In the wake of the reviews following the response to Hurricane Katrina, it is likely that the resource definitions could be expanded to include additional resources, such as an IDMT, that have been needed in response but to date remained undefined.

[56] Proposal was submitted by the Frederick County, MD Sheriff's Office to the Maryland Anti-Terrorism Advisory Council for consideration as part of the FY 2006 Law Enforcement Terrorism Prevention Program (LETPP) grant application process.

[57] U.S. Department of Homeland Security, Federal Emergency Management Agency, *National Mutual Aid and Resource Management Initiative: Glossary of Terms and Definitions* (Washington, D.C.: FEMA, 2005).

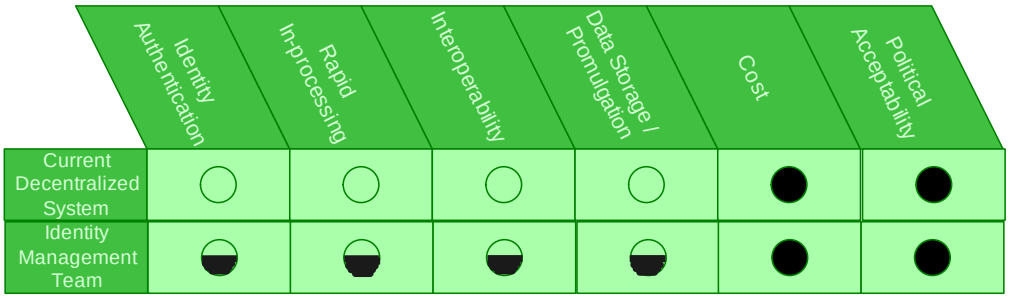

Table 4. Evaluation Matrix: Identity Management Team

E. SUMMARY

The examination of the responses to the 1995 Oklahoma City Murrah Federal Building bombing and the 9/11/01 Attack on the Pentagon revealed lessons learned and the necessary elements to form a defined response resource. The elements were incorporated into the Identity Management Team resource as defined in Table 1. The concept of operations was also defined, as the successful incorporation of the resource is dependent upon operational factors including the establishment of a strong perimeter. The resource demonstration project developed by the Frederick County Sheriff's that was established through the examination of case studies was then evaluated utilizing previously identified criteria for improved terrorism incident response.

The evaluation reveals that the defined Identity Management Team option for improved terrorism incident response is a vital resource; however, it does not stand alone as a complete solution to the identity management problems exposed in the response to previous incidents of terrorism. The IDMT resource definition provides the necessary mechanism to successfully manage on-scene identity allowing for incremental improvement over the response to previous incidents of terrorism. The effectiveness of the resource and terrorism incident management would be bolstered by the implementation of pre-event credentials that allow for rapid identity authentication. The IDMT provides a mechanism to incrementally improve identity management for terrorism incident response. The resource represents a deployable asset that can incrementally improve incident response immediately, while the details and attempts at larger credential standardization solutions are debated.

The need for a dedicated resource for on-scene identity credentialing was further bolstered by the events of Hurricane Katrina. Although the focus of this paper is the response to incidents of terrorism, the Katrina example shows the pervasive identity management capability gap for catastrophic incident response including natural hazards. The report of the House of Representative Select Committee on Hurricane Katrina advised, "The Secret Service was asked by NOPD and the Louisiana State Police to take control of the credentialing process for state and local law enforcement in the New Orleans area. The need for secure credentials for NOPD was a primary concern, as many police officers had lost their official identification badges during the hurricane."[58] The IDMT resource as defined could have served a vital function in response to this catastrophic natural hazard event. This example further evidences the value of the resource as a necessary response asset that can service events beyond terrorism response.

In the context of cost criteria, it must be addressed as to whether this resource is useful for other purposes, or does it just sit and wait for an incident requiring its capabilities. The described development consideration of an IDMT by the Frederick County Sheriff's Office was dual purpose. While the developed resource does close a tremendous gap for the law enforcement responsibility for scene security in the event of an incident of terrorism, it can also serve as a community service by being utilized as the centerpiece of a child identification program. The IDMT mobile resource can be used at fairs, carnivals, and special events to register child information with law enforcement. This serves three purposes: the resource is utilized by and kept operational condition, personnel utilize the equipment and it reinforces initial training, and it provides an additional service to the community. The limited investment is further leveraged in that it provides a resource for incident response and a community asset to capture child identity information, thereby increasing public value.

Table 4 contains a summary of the evaluated criteria for the defined IDMT response resource. The IDMT represents an incremental improvement in identity management for terrorism incident response. The IDMT provides a mechanism to

[58] U.S House of Representatives, Select Bi-Partisan Committee to Investigate the Preparation for and the Response to Hurricane Katrina, *A Failure of Initiative: Final Report of the Select Bi-Partisan Committee to Investigate the Preparation for and the Response to Hurricane Katrina* (Washington, D.C.: GPO, 2006), 256.

monumentally improve identity management when compared to previous catastrophic failures in historical incident response to terrorism, but only trivial in comparison to what is possible.

IV. FIRST RESPONDER IDENTITY SMART CARDS (OPTION 3)

A. OVERVIEW

The option of identity smart cards for first responders is derived from federal identity initiatives. The current federal identity program is driven by the requirements of Homeland Security Presidential Directive-12: Policy for a Common Identification Standard for Federal Employees and Contractors (HSPD-12). HSPD-12 and supporting documents outline an identity paradigm shift from reliance on unverifiable paper credentials to a comprehensive standards based smart card program consisting of identity tokens that can be electronically authenticated. The first responder identity smart card is developed as an option for improved terrorism incident response based on the implementation of this national model for all federal employees and contractors. This chapter provides an overview of smart card technology and the federal HSPD-12 smart card program. Finally, the HSPD-12 program and its application to first responders in the National Capital Region will be evaluated across the identified criteria for its capability to improve terrorism incident response.

1. Smart Card Technology Overview

Smart cards are defined as "plastic devices—about the size of a credit card—that use integrated circuit chips (ICC) to store and process data, much like a computer. This processing capability distinguishes these cards from traditional magnetic stripe cards, which cannot process or exchange data with automated information systems."[59] The card processing capability allows for applications, biometric information, and other data to be stored, encrypted, retrieved, and verified.

There are two basic types of smart cards, contact and contactless. The two terms describe differences in how the ICC is powered and how the data transfer takes place. Contact cards require the direct insertion into an interface device. Contactless smart cards must only be in the proximity of the card reader for information exchange to take place. The transfer of data takes place over radio frequency (RF) waves that are emitted

[59] U.S. Government Accountability Office, *Electronic Government: Federal Agencies Continue to Invest in Smart Card Technology* (Washington, D.C.: GAO, 2004), 1.

through antennae contained in both the card and reader.[60] Hybrid, or multi-technology smart cards, (Figure 2 & 3) may contain both contact and contactless ICC features as well as bar code and magnetic stripe technology. The cards may be manufactured with different integrated chips to serve the specific needs of agencies for physical access control and other applications while maintaining the ability to adhere to interoperability standards.

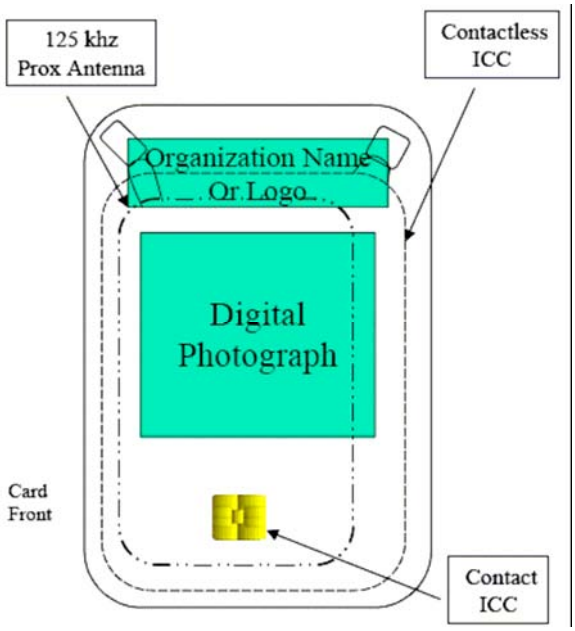

Figure 2. Multi-Technology Smart Card (front)[61]

[60] U.S. General Services Administration, *Government Smart Card Handbook* (Washington, D.C.: GSA, 2004), 16.

[61] Ibid, 27.

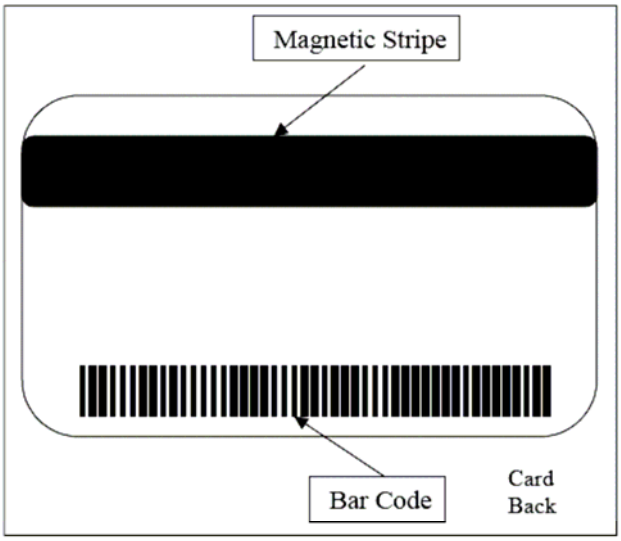

Figure 3. Multi-Technology Smart Card (back) [62]

The smart card provides the capability for an encrypted secure interface and identity verification through the integration of biometric data and remote network verification through public key infrastructure (PKI). PKI is simply "a communications infrastructure that allows users to exchange money and data over the Internet in a secure environment."[63] PKI works on the exchange of information that is encrypted prior to being sent by a public key algorithm then decrypted upon receipt by the certified users private key algorithm. The algorithm is issued along with a digital certificate from the certificate authority (system administration). PKI has many attractive assets for cyber security that allows the user, based on the certificate issued, to access appropriate levels of information and systems. For smart cards, PKI provides a verifiable backbone that can provide a "check" of the card-holder status. PKI allows for a digital certificate to be revoked even though a cardholder is still in possession of the card, therefore, access to physical and logical systems can be rescinded without physical access to the card.

B. FEDERAL IMPLEMENTATION OF SMART CARD TECHNOLOGY

1. Homeland Security Presidential Directive - 12

In Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors, President Bush ordered

[62] U.S. General Services Administration, *Government Smart Card Handbook*, 27.

[63] Ibid, A-6.

all agencies of the United States Government "to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors."[64] HSPD-12 further clarifies secure and reliable identity as consisting of the following criteria.

> Secure and reliable forms of identification for purposes of this directive means identification that (a) is issued based on sound criteria for verifying an individual employee's identity; (b) is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; (c) can be rapidly authenticated electronically; and (d) is issued only by providers whose reliability has been established by an official accreditation process. The Standard will include graduated criteria, from least secure to most secure, to ensure flexibility in selecting the appropriate level of security for each application.[65]

The directive further orders an aggressive program with strict timetables to be implemented based on standards developed by the Secretary of Commerce.

2. Federal Information Processing Standard - 201: Personal Identity Verification

The Secretary of Commerce through the National Institute for Standards and Technology (NIST) released the HSPD-12 directed government-wide standard on February 25, 2005. *Federal Information Processing Standard Publication 201: Personal Identity Verification (PIV) of Federal Employees and Contractors* (FIPS 201) outlines a two stage process to meet the listed criteria for a "secure and reliable form of identification." The stated goal of FIPS-201 is "to achieve appropriate security assurance for multiple applications by efficiently verifying the claimed identity of individuals seeking physical access to Federally controlled government facilities and electronic access to government information systems."[66]

The initial implementation stage, Personal Identity Verification One (PIV-I), includes the description of required processes to meet security and control mandates for

---

[64] *Homeland Security Presidential Directive HSPD-12: Policy for a Common Identification Standard for Federal Employees and Contractors* (Washington, D.C.: The White House, August 2004), 1.

[65] Ibid.

[66] U.S. Department of Commerce, National Institute of Standards and Technology, *Federal Information Processing Standards Publication 201: Personal Identity Verification (PIV) of Federal Employees and Contractors* (Washington, DC: NIST, 2005), 1.

identify proofing of individuals for issuance of federal identification cards under HSPD-12. The federal PIV card will only be issued by accredited agencies and will utilize a process consisting of three necessary components. [67] First, the applicant will personally appear. Second, the applicant will present two forms of identity source documents as certified by the Office of Management and Budget[68] with at least one being issued by a State or Federal authority and submit to necessary biometric screening.[69] Finally, the applicant will be screened through a National Agency Check with Written Inquiries (NACI), Office of Personnel Management (OPM), or National Security community investigation background investigation including fingerprint identification.[70]

The second stage of implementation outlined by FIPS-201, Personal Identity Verification Two (PIV-II), includes the physical and technical elements to support interoperability aspects of HSPD-12. The Federal PIV card bases identity authentication on a three-tiered system. The real-time comparison of biometrics (fingerprint and/or photographic), "something you are", combined with the card itself, "something you have" and PIN numerical "something you know."[71] The tiers backed by the distribution and identity-proofing standards outlined by PIV-I provide a secure identity solution that meets the requirements mandated by HSPD-12. The addition of PKI enabled digital certificate remote network verification architecture provides an additional level of security for both physical and logical access, as the status can be revoked without requiring the physical collection of the PIV card.

The PIV card mandated by FIPS-201 consists of common physical characteristics and appearance elements with allowances for slight variation for specific agency purposes. In an effort to standardize, the physical make-up of the card is consistent with International Organization for Standardization (ISO) and International Electrotechnical

[67] In order to be accredited agencies will be required to implement the guidelines set forth in NIST Special Publication 800-79 Guidelines for Certification and Accreditation of PIV Card Issuing Organizations.

[68] Acceptable identification documents are described on Form I-9, OMB No. 1115-0136 Employment Eligibility Verification.

[69] U.S. Department of Commerce, National Institute of Standards and Technology, *Federal Information Processing Standards Publication 201: Personal Identity Verification (PIV) of Federal Employees and Contractors*, 6.

[70] Ibid.

[71] Ibid., 10-11.

Commission (IEC) requirements. FIPS-201 contains five slightly varied approved models for card fronts and three variations for the back of approved PIV cards. In addition to the ICC standardization aspects the models allow flexibility for the inclusion of magnetic stripe and/ or bar code technology for agency specific applications. Certain fields are mandated on the front of the PIV card such as, name, photograph, affiliation, agency, and expiration date. Required elements on the back of the card include card serial number and agency issuer identification (Figure 4 & 5).

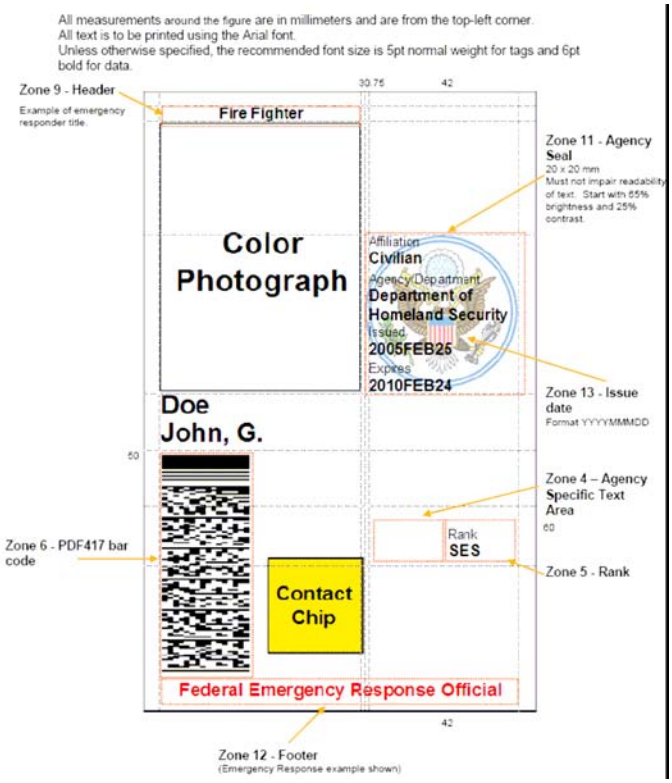

Figure 4. PIV Optional Card Front Data – Emergency Responder[72]

[72] U.S. Department of Commerce, National Institute of Standards and Technology, *Federal Information Processing Standards Publication 201: Personal Identity Verification (PIV) of Federal Employees and Contractors*, 22.

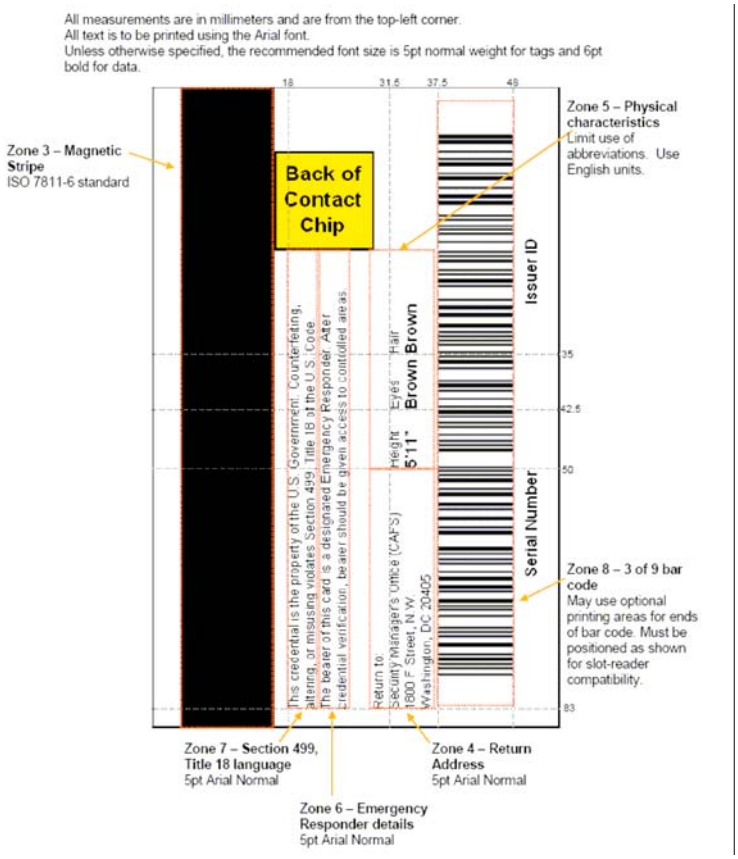

Figure 5. PIV Optional Card Back Data[73]

FIPS-201 (PIV-II) also describes the technical requirements for PIV interoperability, with further detail provided in a series of related NIST and industry technical publications. There are five basic technical requirements governing the federal PIV card. FIPS -201 provides standardization requirements for the ICC, a Card Holder Unique Identifier (CHUID), PIV Card Activation, the PIV authentication data (one asymmetric key pair and corresponding certificate), and biometric data. FIPS-201 requires that the PIV card contain both contact and contactless ICC interfaces. The ICC interfaces are mandated to be consistent with ISO/IEC and *FIPS 140-2: Security*

[73] U.S. Department of Commerce, National Institute of Standards and Technology, *Federal Information Processing Standards Publication 201: Personal Identity Verification (PIV) of Federal Employees and Contractors*, 22.

Requirements for Cryptographic Modules Standards, which when coupled with card reader standardization required by FIPS-201 achieves government-wide interoperability.[74]

The required CHUID must include an expiration date, asymmetric signature field, and Federal Agency Smart Credential Number (FASC-N) that uniquely identifies and tracks each card. The CHUID must be readable from both contact and contactless interfaces. FIPS-201 mandates the specific technical requirements outlined by NIST SP800-73: *Interfaces for Personal Identity Verification* for the CHUID and FASC-N be incorporated into PIV cards. The requirements for the asymmetric signature field must be encoded as a Cryptographic Message Syntax (CMS) as outlined in the Internet Engineering Task Force report RFC 3852 and NIST SP 800-78: *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*.

The PIV card is required to include personal identification number (PIN) based cardholder activation. The PIN must be accepted by the card before it will activate for release of biometric and asymmetric key information. The PIN must meet the standards outlined in FIPS PUB 140-2. The inclusion of a PIN activated system allows for greater card security as the information is not transmitted until a successful contact interface and the correct PIN has been entered.

The PIV card authentication data, must at minimum, consist of one asymmetric private key and a corresponding X.509 public key certificate[75] stored on the card. All keys are accessed only through the contact ICC interface and must not be exportable from the card. The card may also contain additional keys and PKI certificates based on specific agency needs. The X.509 PKI certificate allows for remote network verification through Online Certificate Status Protocol (OCSP) and the Certificate Revocation List (CRL) that must in routine situations be updated by agencies at least every eighteen hours. The inclusion of authentication data allows for the card certificate status to be verified through a secure remote network adding a strong layer of security.

[74] The Associated technical publications include ISO/IEC 7816, ISO/IEC 10373 (1&3), ISO/IEC 14443 (1-4), ISO/IEC 10373 (6), Crypto-Modules FIPS 140-2.

[75] The specifications for X.509 certificates is contained in Federal Identity Credentialing Committee Publication: *X.509 Certificate and CRL Extensions Profile for the Common Policy*.

The final technical requirement of FIPS-201 is the inclusion of biometric data on the PIV card. The following biometric information is collected during the card issuance process: full-set of fingerprints, electronic facial image, and two electronic fingerprints. The full set of fingerprints is not electronically stored and is utilized only for law enforcement background checks. An electronic facial image is printed on the card face and may, but is not required to be, stored on the card. Two electronic fingerprints (right and left index finger) are required to be included on the card for biometric authentication. The technical specification mandates for collection and inclusion of biometric data on the PIV card are located in NIST SP-800-76: *Biometric Data Specification for Personal Identity Verification*.

The federal Personal Identity Verification project mandated by HSPD-12 and described by FIPS-201 provides the basis for a secure identity program far surpassing any current efforts to provide identity management solutions to government employees. The federal program is being implemented in two stages. Under PIV-I the process for identity proofing including background investigations, document requirements, and agency accreditation is administered. The second stage, PIV-2, outlines the technical and interoperability requirements for the federal smart PIV card. The reliance on interoperable smart card technological capabilities such as inclusion of biometric identifiers and encrypted PKI certificates provides identity verification at levels far beyond currently employed solutions (Figure 6). The PIV project and its inherent flexibility provide a secure identity model that can be replicated as a First Responder Identity Smart Card for terrorism incident response applications at the state and local level.

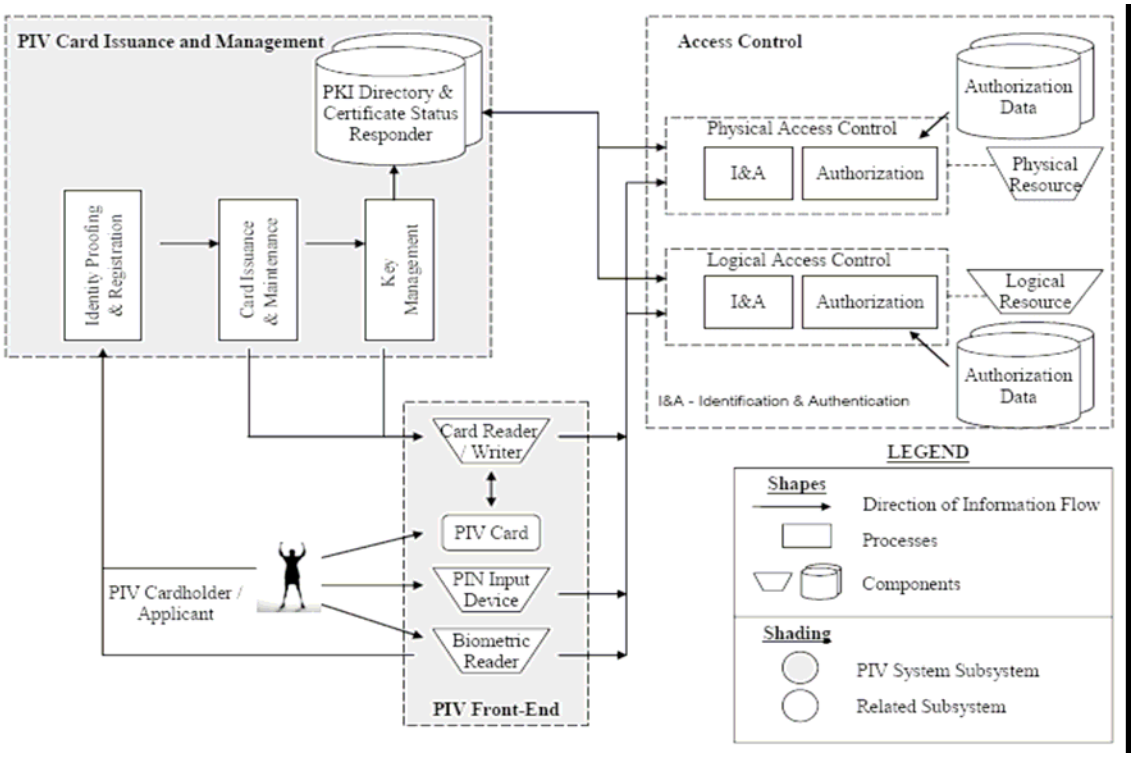

Figure 6. PIV Card System Component Model[76]

C. THE NATIONAL CAPITAL REGION FIRST RESPONDER AUTHENTICATION CARD (FRAC) PROGRAM

The unique multi-jurisdictional nature of the National Capital Region has made it the first region to recognize the need to develop a comprehensive project to implement an HSPD-12/FIPS-201 based identity smart card for first response personnel. The National Capital Region (NCR) consists of the District of Columbia and bordering counties from Maryland and Virginia. HSPD-12 has required Federal Agencies to implement FIPS-201, the standard has not been mandated for implementation by state and local governments. The National Capital Region is the first entity to attempt to replicate the federal program on the State and local level. The blurred lines of federal, state, and local responsibility that is unique to the region makes a common identity standard capable of electronic authentication a necessity. The multi-jurisdictional nature of incident response in the region necessitates a common interoperable platform to authenticate identity and affiliation across levels of government. The NCR project, titled the First Responder

[76] U.S. Department of Commerce, National Institute of Standards and Technology, *Federal Information Processing Standards Publication 201: Personal Identity Verification (PIV) of Federal Employees and Contractors*, 11.

Authentication Card (FRAC), utilizes the standards outlined in FIPS-201 PIV-II to develop a platform capable of interoperability with federally issued smart identity cards.

The NCR FRAC is based entirely on the standards outlined by FIPS-201 PIV-II. One of the major impediments to the implementation of a pure FIPS-201 PIV-I and PIV-II compliant identity card for state and local first responders is the background check requirement. As described in previous sections, FIPS-201 is requires a fingerprint check and National Agency Check with Written Inquiries (NACI) for all personnel to be issued a federal identity credential. The heart of an identity trust model is the security of both the issuance process and the product (token). If the model is vulnerable to infiltration during the issuance process, or the finished product is subject to counterfeit, there is no trust and authentication will be suspect. At the state and local level the cost of conducting FIPS-201 compliant background investigations on all first responders would be exorbitant.

In Frederick County, MD, the example community outlined in Chapter II, only the investigations completed prior to law enforcement employment would meet the standard outlined by FIPS-201. The pre-employment identity verification procedures of other response disciplines including fire, EMS, public works, public health, and clinical care would not meet the standard. In order to meet PIV-I enrollment standards, additional investigation of employees would be required. This raises numerous concerns ranging from personal privacy to the significant additional associated costs. The NCR FRAC has addressed this problem by delineating levels of authentication based on the scope of enrollment procedures. This allows for a graduated trust model where four increasing levels of authentication are defined based upon the depth of procedures prior to credential issuance. It does not preclude agencies with minimal procedures from inclusion in the program; however, when the card is electronically authenticated the level of authentication is displayed allowing the user to determine if additional scrutiny is necessary. The graduated model ensures maximum participation among local governments, due to limited additional financial commitments, while maintaining trust.

The NCR was ground-zero for a terrorist attack on 9/11/01. The response to the Pentagon revealed a pervasive this identity gap, as documented in previous chapters. In

addition, the NCR also has the unique frequent need for identity authentication of first responders from dozens of agencies across all levels of government for daily operations. The FRAC is a necessary element in the NCR for both daily operations and the response to critical incidents such as those created by terrorist attack.

The NCR FRAC program is moving through the research and evaluation stage. In February 2006, exercise the interoperability through a limited enrollment and multi-jurisdictional exercise dubbed "Winter Fox." The interoperability and authentication capability was targeted by the exercise that took place in four locations including the Pentagon, Port of Baltimore, Virginia Department of Transportation, and Frederick County, MD. The exercise sought to examine the ability electronically validate PKI certificates of FIPS 201 standardized smart card through four different back end architectures. The cards included in the exercise included the NCR FRAC, Maryland FRAC, Transportation Security Administration Transportation Worker Identity Credential (TSA TWIC), and the Department of Defense Common Access Card (DoD CAC). Each of the identified cards are maintained through different back-end infrastructures. The exercise sought to test the capability to validate personnel identity across the disparate infrastructures.

The exercise utilized hand-held readers that received satellite data regarding certificate revocation every 24 hours. The readers were utilized to read and validate PKI enabled FIPS-201 smart cards. The Winter Fox exercise resulted in 285 scans of the smart cards with disparate back end architectures. Of the scans, 79 resulted in PIN verification failures.[77] This means that 28% of the attempts were unable to be validated by the back-end architecture because of incorrect PIN entry, or more simply cardholder error. The 206 scans where the user did not error in PIN entry resulted in 100% validation. This provides strong evidence of the interoperable capability of FIPS smart cards. The hand-held reader also has the ability to read, but not validate, 2D barcodes contained on most driver licenses. Several driver licenses were read, but not validated as part of the exercise.

[77] Craig Wilson, "Winter Fox Interoperability Demonstration" (presentation at the meeting of the Government Smart Card Interagency Advisory Board, 15 March 2006), 14, http://www.smart.gov/iab/presentations/IABmeetingMarch2006.pdf. (accessed 18 August 2006).

D. EVALUATIVE CRITERIA

The utilization of FIPS-201 standards with the NCR FRAC program and preliminary evaluation through the Winter Fox exercise, demonstrates the capability to institute a government-wide trust model for identity authentication. The results of the exercise show promise for improvement of identity management during the response to large-scale terrorism incidents. The FIPS-201/ NCR FRAC will be evaluated utilizing the incident response criteria as developed in Chapter I. The criteria include identity authentication, rapid in-processing, interoperability, and data storage/ promulgation. In addition, the traditional public policy criteria of cost and political acceptability will be examined.

The first element of the criteria for improved terrorism incident response is identity authentication. Identity is able to be authenticated if a trust model is developed that allows for verification. Trust is developed by ensuring both issuance process and product are sound and strongly resistant to exploitation. The PIV-I enrollment model outlined by FIPS-201 is resistant to exploitation through required background investigations and consistent processes. The NCR/ FRAC interpretation allows for levels of enrollment based on the intrusiveness of enrollment procedures. This represents a vast improvement in identity proofing from the current system outlined in Chapter II. The issuance process, combined with the smart card standards required by FIPS-201 PIV-II provides a complete model of secure process and product. The standards base allows identity to be verified through PKI remote electronic verification. The FIPS-201/ NCR FRAC card is capable of being read by handheld readers that can instantly check the authenticity of the card. Followed by user PIN entry, the card can be checked against the PKI directory and the certificate status responder to reveal the current status of the credential. The biometric digital fingerprints stored on the card can also be utilized through a reader to further authenticate identity. The three-tiered system (something you are, something you have, and something you know) of the PIV program provide a level of identity authentication that has not previously existed for terrorism incident response. A government-wide smart card initiative will provide the instant identity verification

necessary for efficient terrorism incident response and provide a countermeasure to prevent the terrorist/ impostor from infiltrating secure scenes through unverifiable paper credentials.

The second element of the criteria for improved terrorism incident response is rapid in-processing. The current identity system requires additional identity checks and issuance of on-scene identity credentials, whether by computer generated card, wrist-band, or other platform that causes lengthy delays for on-scene in-processing. The NCR FRAC eliminates confusion and delays and allows responders to get work on the problem. Personnel identity can be verified and in-processed through a remote card reader that does not take longer to authenticate than the traditional flash identification and routine questions that follow. The FIPS-201/ NCR FRAC would eliminate the lengthy delays to get responders credentialed and into the incident scene. The hand-held validation device utilized in the NCR Winter Fox exercise required the card to be placed in the device and the PIN entered by cardholder, resulting in instant verification. The FIPS-201/ NCR FRAC provide a solution that allows for strong identity authentication without sacrificing the need for rapid in-processing of personnel.

The third element of the criteria for improved terrorism incident response is interoperability. FIPS-201 creates a standards based solution to identity management. The smart card standards outlined in PIV-II allow for interoperability among identity tokens because they all meet the same technological standards. The NCR Winter Fox exercise successfully demonstrated that standards based smart cards with disparate back-end infrastructures could be authenticated. During the exercise, cards issued by the Federal Government (Department of Defense, Department of Homeland Security, and Transportation Security Administration) could interoperate with those issued by a State (MD FRAC). The FIPS-201 standard provides the interoperable basis necessary to authenticate identity from various response disciplines and different levels of government. The FIPS-201 standard allows for interoperability necessary to improve terrorism incident response.

The fourth element of the criteria for improved terrorism incident response is data storage/ retrieval and promulgation capability. The technical capabilities of the FIPS-

201/ NCR FRAC smart card allow data to be transferred from the card providing the ability to make information on responders immediately available to on-scene command. Although not documented in FIPS-201, the smart card capability exists to include training qualification data. As additionally identified personnel standards are developed under the National Incident Management System, those definitions can be included on the card (Firefighter I, Firefighter II, etc.). Once developed, these standards will allow more information to be delivered to on-scene command following card and PIN entry in remote handheld devices. The FIPS-201 smart card provides the capability to improve terrorism incident response through the ability to store and retrieve data related to personnel responding to an incident of terrorism. This would provide the incident commander with information to answer the critical questions of "Who is this?" and "What can they do for me?"

The traditional public policy concerns of cost and political acceptability are the final elements to evaluate solutions for improved terrorism incident response. These criteria balance the theoretical problem solution against the financial requirements and willingness of political entities to implement the solution. The public policy criteria bring the reality of government prioritization and choice based on budgetary constraints and political will. These criteria temper the seemingly perfect solution to the identified problem with realities of the requirements for governmental action.

The FIPS-201/ NCR FRAC presents the option with the greatest implementation cost. The current decentralized system presented in Chapter II requires no additional financial investment, as it is currently operated in some capacity by every level of government. The Identity Management Team option presented in Chapter III requires a moderate investment of approximately $140,000. The following table (Table 5) appeared in the April 2001 U.S. General Services Administration (GSA) publication *CIO/ PKI Smart Card Project: Approach for Business Case Analysis of Using PKI on Smart Cards for Governmentwide Applications*.[78] The table outlines a cost estimate for PKI Smart Cards with biometrics for a notional agency issuing 10,000 cards and includes 1,000 readers for physical building access and 10,000 network readers for logical access. These

[78] U.S. General Services Administration, *CIO PKI/Smart Card Project: Approach for Business Case Analysis of Using PKI on Smart Cards for Governmentwide Applications* (Washington, D.C.: GSA, 2001).

options are presented in the publication as comprehensive solutions to identity management for identity authentication and protection of physical and logical governmental assets. The costs are based on FY 2001 estimates.

Option D - Agency Opts for PKI/Smart Cards and Biometrics					
		Unit Cost	**Quantity**		**Total Cost**
Cost of tokens	$	15	10,000	$	150,000
Cost of network readers	$	125	10,000	$	1,250,000
Cost of building access readers	$	200	1,000	$	200,000
Cost of infrastructure	$	300,000		$	300,000
Cost of issuing certificates	$	125,000		$	125,000
Total Cost of Option D (constant dollars)				***$***	***2,025,000***

Table 5. Total Costs for PKI/ Smart Cards and Biometrics for Notional Agency[79]

The use of FY 2001 cost estimates would intuitively lead to the conclusion that costs would be significantly higher for FY 2007 implementation. The application of Moore's law to the problem concludes that the costs of would decrease because of the rapid advance of technology and lower costs of production.[80] The cost of smart cards has decreased. According to the February 2004 GSA *Government Smart Card Handbook* the cost per card is listed between $3 and $10 depending on card capabilities as compared to $15 in the FY 2001 estimate.

Utilizing Frederick County, MD as described in Chapter II for a baseline, implementation costs are below $500,000 (Table 6). Frederick County has fewer employees than the estimate provided for the notional agency in the GSA publication. The table below (Table 6) represents the costs associated with implementation for the example community with approximately 2,500 employees. The example community has an FY 2006 operating budget of approximately $361,000,000, a total investment in smart card technology would represent 0.1% of the total budget.

[79] U.S. General Services Administration, *CIO PKI/Smart Card Project*, 4-8.

[80] Gordon E. Moore, "Cramming More Components onto Integrated Circuits," *Electronics*, 19 April 1965.

Frederick County, MD: PKI / Smart Cards and Biometrics					
		Unit Cost	Quantity		Total Cost
Cost of Tokens	$	10	2500	$	25,000
Cost of Network Readers	$	125	2500	$	312,500
Cost of Building Access Readers	$	200	250	$	50,000
Cost of Infrastructure	$	75,000		$	75,000
Cost of Issuing Certificates	$	31,250		$	31,250
Total Cost of Implementation				$	493,750.00

Table 6. PKI/ Smart Cards Implementation Estimate: Frederick County, MD

The total cost of implementing PKI enabled smart cards is significant, but not cost prohibitive. Not accounted for in the estimates above are the costs associated with the existing identity system. When factoring in the costs associated with the legacy system, although likely not significant, the implementation costs are slightly reduced. As is true for most municipal governments, identity management is not a consolidated function, does not exist as a budgetary line item, and is absorbed in operating costs, therefore, a total expenditure is difficult to ascertain. In addition to the cost of the legacy system, leveraging federal grant funds available through the State Homeland Security Grant Program and Law Enforcement Terrorism Prevention Program can supplement a local investment lessening the local budgetary impact.

The cost of background investigations is also not included in the implementation costs. The NCR FRAC solution related to levels of authentication based on depth of investigation, is the preferred option as opposed to the FIPS-201 PIV-I requirements. The costs of PIV-I background investigation requirements would be exorbitant for local governments, making smart card implementation unattainable. The NCR FRAC program leveled determination presents a common sense solution to identity authentication that balances security, fiscal responsibility, and political acceptability.

The final element of the criteria for evaluation is political acceptability. As stated in previous chapters, cost is often intertwined with political acceptability. In the case of the FIPS-201/ NCR FRAC this is also true. The program also raises privacy concerns that could potentially impact the acceptability of the option. There are also additional concerns related to the method of implementation for a nationwide program that can

affect the program acceptability. Although the program has not been designed, the method of implementation, whether by mandate or voluntary compliance, can impact state and local government willingness to accept the program.

The key component as it relates to the cost/ political acceptability is increasing public value. The outlined FIPS-201/ NCR FRAC option adds value in that it provides solutions to many of the problems associated with terrorism incident response, but it also provides additional benefits to terrorism prevention and protection missions, and cost saving to other government operations. The smart card option provides the opportunity for vastly improved protection of physical and logical assets, and increases overall government efficiency.

The FIPS-201/ NCR FRAC smart card option provides additional benefits through the ability to improve physical access control at government facilities nationwide. The United States General Accounting Office report *Security: Breaches at Federal Agencies and Airports* details the success of undercover agents in penetrating nineteen federal buildings and two commercial airports without screening, through the use of fraudulent law enforcement credentials. The report states "At the 21 sites that our undercover agents successfully penetrated, they could have carried in weapons, listening devices, explosives, chemical/biological agents, devices, and/or other such items/materials."[81] The report details another dimension of the identity management capability gap that can be addressed by the broad application of credentials capable of electronic authentication. This is possible through the implementation of PKI enabled smart card technology for the protection of critical infrastructures. A comprehensive identity management program utilizing FIPS-201/ NCR FRAC smart card technology will prevent those agents or terrorists of the future from penetrating secure sites through unverifiable fraudulent credentials.

The FIPS-201/ NCR FRAC option also provides the ability to improve information system security through incorporating card readers into computer access. Incorporated with physical access control the system provides two layers of security for logical systems. The first hurdle for a potential assailant is entering the physical location;

[81] U.S. General Accounting Office, Office of Special Investigations, *Security: Breaches at Federal Agencies and Airports* (Washington, D.C.: GAO, 2000), 3.

then, the computer card reader option provides a second level of security. An incorporated smart card option decreases the potential for cyber attack through on-site infiltration through this two-layer process.

The FIPS-201/ NCR FRAC option also provides benefits to other government operations. The *CIO/ PKI Smart Card Project: Approach for Business Case Analysis of Using PKI on Smart Cards for Governmentwide Applications* identifies that implementing smart card technology with digital forms improves efficiency "reduces paperwork, eliminates redundant data entry, and improves data accuracy as transcribing and data entry errors are eliminated"[82] A smart card based system implemented with e-government initiatives creates public value and cost savings in other areas of government processes. The many additional benefits of the implementation of smart card technology address concerns of cost relative to the public value it creates.

Other elements of a FIPS-201/ NCR FRAC based smart card program that raise political acceptability concerns are the issues of personal privacy and the method of implementation. The enrollment process, storage of data, and access to data are concerns that will be raised by privacy advocates relative to the implementation of a smart card based program. The technical specifications of the card as outlined by FIPS-201 PIV II, including the requirement for PIN activation through a contact reader for data retrieval, provides for data protection on the card. The larger concerns come from the storage of data gathered through the enrollment process. The interoperable nature of the standards based system allows for the data to be housed with the host organization, easing concerns of national information databases. In order to fully address these concerns, stringent policy must be in place prior to implementation. In development of the Transportation Worker Identity Credential (TWIC) program the Transportation Security Administration developed a Privacy Impact Assessment that describes the protections. The following is an excerpt.

> All collected data will be electronically stored in one location, and no paper copies will be maintained. The data collected during enrollment will be encrypted before transmission and then transmitted to the TSA system over a secure internet connection. The data is then automatically deleted from the Trusted Agent enrollment workstation. Once the information is

[82] U.S. General Services Administration, *CIO PKI/Smart Card Project*, 5-6.

> sent to TSA, the information will be forwarded to the various interfaces to conduct the security threat assessment. After the card production facility produces the credential, the data will be automatically deleted from the card production facility system. Personal information collected will not be stored outside the TSA system except when it is actually being used by other parts of the system.[83]

The TSA program addresses concerns by describing its data security measures. In order for a FIPS-201 /NCR FRAC model program to be accepted by state and local governments, these type of assurances must be developed.

The final dimension of political acceptability is the method of implementation. The FIPS-201 model is a requirement of federal government agencies under HSPD-12. This is well within the power of the President to require action by federal agencies. In the NCR, the FIPS-201 base model with local modification of PIV-I requirements was by necessity and choice. The NCR has dedicated a portion of its Urban Area Security Initiative (UASI) funds to develop the project after recognizing its importance. The development of a nationwide program must follow a similar pattern. The standards and best practices for implementation must be available for review and adoption by interested governments. The issue is critically important; however, it will not be successfully implemented by force from the federal government.

The federal government can initially encourage adoption through grants and the recognition of secure identity solutions for first responders as a national priority through inclusion as a future focus area of the National Preparedness Goal. The lessons learned from the nationwide federal agency implementation of HSPD-12 / FIPS-201 will be critical to successfully launching a national voluntary program to improve first responder identity. To prescribe the implementation of such a program at the state and local level without the benefit of the federal government implementation experience would be senseless and lead to waste. The implementation of the federal program will reveal best practices and lessons learned that will provide the roadmap to success. In addition, programs such as the NCR FRAC provide guidance for the development of identity standards and a trust model that makes sense for state and local governments.

[83] U.S. Department of Homeland Security, Transportation Security Administration, *Privacy Impact Assessment for the Transportation Worker Identification Credential Program* (Arlington, VA: TSA, 2006), 6.

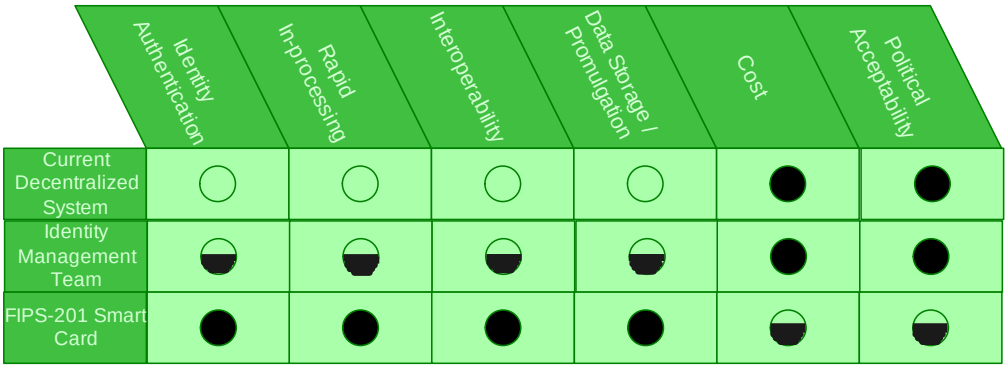

Table 7. Evaluation Matrix: FIPS 201/ NCR FRAC Smart Card

E. SUMMARY

This chapter details the smart card technology option for improving first responder identity management for terrorism incident response. The technology is reviewed and two specific smart card technology programs further explored. The federal program under HSPD-12 is detailed including the guiding technical document FIPS-201. The local implementation of a FIPS-201 based First Responder Authentication Card in the National Capital Region is also examined.

The evaluation of smart card technology under the FIPS-201/ NCR FRAC models revealed its vast capability to improve terrorism incident response. Smart card capabilities to perform identity authentication, rapid in-processing, interoperability, and data storage/ promulgation ability provide it with the necessary attributes to vastly improve terrorism incident response. The questions of public policy, however, temper the clear choice for incident response improvement with concerns related to cost and political acceptability. Concerns related to the overall cost were examined and revealed that despite higher implementation investment, the option increases public value. Smart standards based smart card technology provides additional benefits to the protection of physical and logical assets from terrorism. It also allows for the implementation of e-government initiatives that can increase overall efficiency of government, thereby increasing public value. The areas of concern related to political acceptability include both privacy and the method of implementation. The privacy concerns are addresses

through two mechanisms. First, the technical specifications of the smart card provides for data security. Second, the concerns related to data security collected through the enrollment process will need to be addressed through strong policies related to access and data security as provided through the example of the TSA TWIC program.

Standards based smart card technology for the identity of first responders has the ability to improve incident response and provide benefits to other aspects of government operations. The technology as part of a larger systems approach to identity has the capability to authenticate on-scene identity and facilitate on-scene identity management needs including personnel accountability, jurisdictional reimbursement, and personnel compensation. As with many aspects of Homeland Security this is only a part of the overall problem of identity management for terrorism incident response. The key questions for incident commander as identified in earlier chapters of "who are you?" and "what can you do for me" lie beyond the capabilities of technology and require political agreement and a willingness to improve overall preparedness. Smart cards provide the capability to store data, but the definitions of the data and what it will mean to on-scene commanders will require additional coordination and the recognition of the need for change.

V. CONCLUSIONS AND RECOMMENDATIONS

In his book *Alice in Wonderland*, author Lewis Carroll wrote, "If you don't know where you are going, then it does not matter which road you take." The previous chapters serve as the initial survey for a new road to the future of identity management for terrorism incident response. The course is defined by examining how identity management has failed in the previous response to incidents of terrorism, and how it will fail in the future without a concerted effort to engage deficiencies. The future requires problem recognition, field evaluation, and a decisive course toward a future vision. Understanding the deficiencies of the past and breaking the identity management cycle of failure that appears again and again in our after-action recommendations and "lessons learned" is critical to our future success.

Methods are needed to manage the two distinct aspects of identity as they relate to response to incidents of terrorism. The question of identity hinges on definitional aspects. First, is "the collective aspect of the set of characteristics by which a thing is definitively recognizable or known."[84] Second, is "the set of behavioral or personal characteristics by which an individual is recognizable as a member of a group."[85] Essentially it comes down to, "how do we know you are you?" and "how do we know your affiliation and what you can do?" These definitional aspects transfer to terrorism incident response in the two key answers needed by on–scene commanders managing personnel in responding to incidents of terrorism. The key questions as identified in Chapter I are "Who is this?" and "What can they do for me?" These key questions are necessary in any incident response; however, in the response to an incident of terrorism and the threat of secondary attack the question "who is this?" requires a follow up question of "is this a friend or enemy?" The nature of incident response requires a process that provides trusted answers rapidly.

The evaluation of presented alternatives leads to a conclusion requiring another literary reference. The alternatives are not unlike the bowls of porridge in the childhood

[84] *American Heritage Dictionary*, "Identity."

[85] Ibid.

fairytale story of Goldilocks and the Three Bears. They are too hot, too cold, and just right. The problem lies in which lens you use to examine the problem, or check the temperature. The terrorism incident response criteria, absent public policy considerations, presents an obvious choice, conversely public policy concerns absent incident response improvement criteria also presents an obvious but different choice. The federal government under HSPD-12 has defined the future of identity, providing the destination. The road to get there for local governments has yet to be paved and is filled with potholes and detours. The journey will be long and hard, but the trip will be worthwhile.

There are no strong arguments for the status of identity at the state and local level to remain unchanged. The current system provides little in the way of public value and no benefit to terrorism incident response. It also provides little protection of physical and logical assets. It exists simply because of its low cost. It is broken, so it is time to fix it. The federal government has recognized this problem evidenced by HSPD-12 and the FIPS-201 smart card program. The course has been set for the federal government, as it will issue smart cards to more than two million federal civilian employees and contractors, supported by the more than five million already issued by the Department of Defense to members of the armed forces and their dependents.

The federal effort as described in HSPD-12 sets its identity standard with the goals "to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy." As revealed by the analysis in Chapter IV, it can also serve to vastly improve terrorism incident response. The challenges for state and local governments, as revealed through the evaluation of public policy criteria, do not outweigh the public benefit of a standards based system that allows for interoperability between levels of governments, vastly improves terrorism incident response, increases physical and logical protection of assets, and provides a mechanism for increased government efficiency. The construct of identity for first responders must change. The identity characteristics of "flash" identification, vehicle, uniform, and a demeanor consistent with position must be exchanged for secure identity tokens and verification. The risk is too great for the paradigm to remain unchanged.

The following represent recommendations for the path toward improved terrorism incident response.

1. Develop an Identity Management Team (IDMT) as typed resource for incident response

The implementation of a nationwide interoperable identity solution will take years and will likely never achieve complete participation by all state and local jurisdictions. On-scene identity management is a current capability gap that must be addressed. The IDMT can serve to make improvement toward closing this gap in a formalized way. The IDMT resource definition, developed out of the on-scene experience of responders who instituted ad-hoc systems from available materials, provide lessons for an incremental improvement. The great leap forward presented by the FIPS-201/ NCR FRAC option will take years to implement. Although not a complete solution, the IDMT is an option that can be immediately implemented to provide a modest improvement to identity management for terrorism incident response. The IDMT resource definition developed in Chapter III presents a starting point to be further developed and refined through evaluation and exercise.

The Secretary of the Department of Homeland Security should task the U.S. Secret Service (USSS) with the development of the resource definition and equipment recommendations. The USSS experience in providing credentialing support to countless National Security Special Events and the responses to both the 9/11 attack on the Pentagon and Hurricane Katrina places it in the unique position of knowing the most about this problem. The identity management capability gap for terrorism incident response needs both an immediate and long-term solution. The IDMT represents a short term option for incremental improvement in terrorism incident response and should be further developed.

2. Develop personnel credentialing standards for all response and recovery disciplines.

The Coordinating Agency for each of the fifteen Emergency Support Functions (ESF) identified in the National Response Plan should develop credentialing standards for personnel in conjunction with State and local partners. Those responsible for the

function should be required to develop the definition of qualifications necessary to deliver services within its functional area. The efforts of the U.S. Department of Health and Human Services through its ESAR-VHP program have resulted in credentialing standards for personnel in ESF #8 Public Health and Medical Services. The program should be replicated by the other ESF areas to ensure preparedness and capability to deliver services in the event of a terrorist incident or other catastrophic event.

The NIMS Integration Center has begun the process of creating credentialing standards for certain job titles. These areas include incident management, emergency medical services, fire/HazMat, law enforcement, medical and public health, public works, search and rescue, and animal health emergencies response. The NIMS Integration Center should serve as the clearinghouse for the final product; however, the development should be tasked to those responsible for delivery of the function in the time of crisis. Development by ESF ensures that critical mission areas will not be overlooked and develops accountability, as the ESFs represent the range of services needed to respond to a crisis. Accountability is developed as the failure to engage the credentialing question creates an avenue for post-incident scrutiny for the ESF lead.

3. Develop Model Communities and e-government Best Practices Utilizing FIPS-201 / NCR FRAC framework.

The development of FIPS-201 / NCR FRAC identity tokens at the state and local level will require testing, evaluation, and best practices. This can be accomplished by developing model communities. The NCR FRAC is one example although full implementation has not yet been achieved. The NCR represents a major city program, it also must be replicated in suburban and rural communities to show its applicability. The goals of the model communities will be to develop best practices through integration of smart card capabilities to develop e-government initiatives that increase efficiency and streamline processes. The cornerstone to national acceptance will be the public value that is created through more efficient government. In addition to the obvious benefits to terrorism protection, prevention, and response missions, the capabilities of smart cards represent an opportunity for a revolution in government administration.

The model communities will also test incident response capabilities of the cards. Through exercise, the data definitions needed to support incident response can be developed and refined. Emergency Assistance Compact (EMAC) assistance can also be exercised between the model communities to evaluate interoperability for catastrophic response. The best practices developed in model communities for both routine government processes and incident response will be the keys to future success.

4. Develop National Rollout model based on successful local implementation.

The developments and best practices of the model communities will drive national implementation. The lessons learned from the model communities will be incorporated and refined to develop a final product for national implementation. The framework and processes can be developed, but the program implementation must remain a local government option.

5. Add Identity Management as a capability specific priority of the National Preparedness Goal.

The Interim National Preparedness Goal currently identifies overarching and capability specific priorities. The three overarching priorities include implementing the National Incident Management System and the National Response Plan, expanded regional collaboration, and implementation of the National Infrastructure Protection Plan. The four capability specific priorities include strengthening information sharing and collaboration, interoperable communications, CBRNE detection, response, and decontamination, and medical surge and mass prophylaxis. The credentialing standards developed by the ESF groups and the national rollout model derived from best practices in example communities will provide the road map for implementation. The inclusion of Identity Management as a national priority will provide a focus and allow communities to develop the model locally, leveraging federal homeland security funding with legacy system costs to aid implementation.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

AP Foreign Desk. Excerpts from the Reagan Interview with 4 Correspondents. *New York Times*, 4 December 1987.

Bardach, Eugene. *A Practical Guide to Policy Analysis: The Eightfold Path to Effective Problem Solving*. Washington, D.C.: CQ Press, 2005.

City of Oklahoma City. *Alfred P. Murrah Federal Building Bombing April 19, 1995: Final Report*. Stillwater, OK: Fire Protection Publications, 1996.

Cook, Meghan, Mark LaVigne, Christina Pagano, Sharon Dawes, Theresa Pardo. *Making a Case for Local E-Government*. Albany, NY: SUNY University at Albany, Center for Technology in Government, 2002.

Dawes, Sharon S., Thomas Birkland, Giri Kumar Tayi, Carrie A. Schneider. *Information, Technology, and Coordination: Lessons from the World Trade Center Response*. Albany, NY: University at Albany, SUNY, Center for Technology in Government, 2004.

Federal Emergency Management Agency. United States Fire Administration. *Responding to Incidents of National Consequence: Recommendations for America's Fire and Emergency Services Based on the Events of September 11, 2001 and Other Similar Incidents*. Washington, D.C.: FEMA, 2004.

———. *The World Trade Center Bombing: Report and Analysis*. Emmitsburg, MD: USFA, 1993.

Federation for Identity and Cross Credentialing Systems. Welcome To Fixs. Accessed 9 June 2006. Available from http://www.fixs.org/.

Goldman, Roger L. and Steven Puro. Revocation of Police Officer Certification: A Viable Remedy for Police Officer Misconduct?. *St. Louis University Law Journal* 45, no. 541 (Spring 2001).

Gordon, Gary R., and Norman A. Wilcox. *Identity Fraud: A Critical National and Global Threat*. Utica, NY: Utica College, Economic Crime Institute, 2003.

Haberstroh, Joe and Steve Wick. Military Impostor Fools Coast Guard. *New York Newsday*, 27 July 1996.

Homeland Security Act. U.S. Code Annotated. Vol. 6 sec. 101 (2002).

Houghton, Brian and Jonathan Schacter. Coordinated Terrorist Attacks Implications for Local Responders. *FBI Law Enforcement Bulletin* 74, no. 5 (May 2005). Accessed 15 January 2006. Available from htttp://www.fbi.gov/publications/leb/2005/may2005/may05/leb.htm#page11/.

Lux, Larry. The Impact of Homeland Security Presidential Directive 5 on the Public Works Community. *American Public Works Association Reporter Online*, January 2005. Accessed 14 May 2006. Available from http://www.apwa.net/Publications/Reporter/ReporterOnline/index.asp?DISPLAY=ISSUE&ISSUE_DATE=012005&ARTICLE_NUMBER=960/.

McKinsey and Company. *Improving NYPD Emergency Preparedness and Response*. New York, NY: McKinsey and Company, 2002.

Moore, Gordon E. Cramming More Components onto Integrated Circuits. *Electronics*, 19 April 1965, 114-117.

National Memorial Institute for the Prevention of Terrorism. *Oklahoma City- Seven Years Later: Lessons Learned for Other Communities*. Oklahoma City, OK: MIPT, 2002.

National Registry of Emergency Medical Technicians. About EMS. Acessed 9 April 2006. Available from http://www.nremt.org/about/ems_learn.asp/.

National Commission on Terrorist Attacks Upon the United States. *Staff Statement No. 14*. n.p., n.d.

———. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*. Washington, D.C.: GPO, n.d.

National Fire Protection Association. *Standards for Fire Service Professionals*. Quincy, MA: NFPA, 2006.

Titan Systems Corporation. *Arlington County: After Action Report on the Response to the September 11 Terrorist Attack at the Pentagon*. n.p., n.d.

United States Const., Amendment X

U.S. Department of Commerce. National Institute of Standards and Technology. *Biometric Data Specification for Personal Identity Verification*. Gaithersburg, MD: NIST, 2005.

———. *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*. Gaithersburg, MD: NIST, 2005.

———. *Guidelines for the Certification of PIV Card Issuing Organizations*. Gaithersburg, MD: NIST, 2005.

———. *Federal Information Processing Standards Publication 201: Personal Identity Verification (PIV) of Federal Employees and Contractors*. Washington, DC: GPO, 2005.

U.S. Department of Health and Human Services. Health Resources and Services Administration. *Emergency System for Advance Registration of Volunteer Health Professionals Program: Interim Technical and Policy Guidelines, Standards and Definitions*. Washington, D.C.: HRSA, 2005.

U.S. Department of Homeland Security and Federal Bureau of Investigation. *Information Bulletin: Potential Terrorist Use of Public Safety or Service Industry Uniforms, Identification, or Vehicles*. Washington, D.C.: DHS, 2004.

U.S. Department of Homeland Security. Federal Emergency Management Agency. *National Mutual Aid and Resource Management Initiative*. Washington, D.C: FEMA, 2005.

———. *Typed Resource Definitions: Law Enforcement and Security Resources*. Washington, D.C.: FEMA, 2005.

U.S. Department of Homeland Security. *National Incident Management System*. Washington, DC: GPO, 2004.

U.S. Department of Homeland Security Safecom Program. Interoperability. Accessed 14 July 2006. Available from http://www.safecomprogram.gov/SAFECOM/interoperability/default.htm.

U.S. Department of Homeland Security. Transportation Security Administration. *Privacy Impact Assessment for the Transportation Worker Identification Credential Program*. Arlington, VA: TSA, 2006.

U.S. General Accounting Office. *Electronic Government: Challenges to the Adoption of Smart Card Technology*. Washington, D.C: GAO, 2003.

U.S. General Accounting Office. Office of Special Investigations. *Security: Breaches at Federal Agencies and Airports*. Washington, D.C.: GAO, 2000.

U.S. General Services Administration. *CIO PKI/Smart Card Project: Approach for Business Case Analysis of Using PKI on Smart Cards for Governmentwide Applications*. Washington, D.C.: GSA, 2001.

———. *Government Smart Card Handbook*. Washington, D.C.: GSA, 2004.

U.S. Government Accountability Office. *Electronic Government: Federal Agencies Continue to Invest in Smart Card Technology*. Washington, D.C.: GAO, 2003.

U.S. House of Representatives, Select Bi-Partisan Committee to Investigate the Preparation for and Response to Hurricane Katrina. *A Failure of Initiative: Final Report of the Select Bi-Partisan Committee to Investigate the Preparation for and the Response to Hurricane Katrina*. Washington, D.C.: GPO, 2006.

The White House. *Homeland Security Presidential Directive HSPD-8: National Preparedness*. Washington, D.C: The White House, 2003.

———. *Homeland Security Presidential Directive HSPD-12: Policy for a Common Identification Standard for Federal Employees and Contractors*. Washington, D.C.: The White House, 2004.

Wilson, Craig. Winter Fox Interoperability Demonstration. presented at the Government Smart Card Interagency Advisory Board. 15 March 2006. Accessed 18 August 2006. Available at http://www.smart.gov/iab/presentations/IABMeetingMarch2006.pdf.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Dr. Robert Bach
   Center for Homeland Defense and Security
   Naval Postgraduate School
   Monterey, California

4. Mr. Anthony Cieri
   Cieri Consulting Group Inc.
   Philadelphia, Pennsylvania

5. Sheriff James W. Hagy
   Frederick County Sheriff's Office
   Frederick, Maryland